NAVAL FACILITIES ENGINEERING SERVICE CENTER
Port Hueneme, California 93043-4370

USER'S GUIDE
UG-2040-SHR

USER'S GUIDE ON CONTROLLING LOCKS, KEYS AND ACCESS CARDS

DoD Lock Program

Naval Facilities Engineering Service Center

1100 23rd Ave.

Port Hueneme, CA 93043

July 2000

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-018

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 2000	Final; FY99 - FY00

4. TITLE AND SUBTITLE
USER'S GUIDE ON CONTROLLING LOCKS, KEYS AND ACCESS CARDS

5. FUNDING NUMBERS

6. AUTHOR(S)
Eric Elkins and Mike Farrar

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSE(S)
Naval Facilities Engineering Service Center
1100 23rd Ave.
Port Hueneme, CA 93043-4370

8. PERFORMING ORGANIZATION REPORT NUMBER
UG-2040-SHR

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESSES
Chief of Naval Operations (N09N3)
Washington Navy Yard
716 Sicard Street, SE, Bldg 111
Washington, DC 20388-5380

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This user's guide provides information and recommended procedures for establishing key and lock programs. Also included are specific hardware requirements for protection of arms, ammunition, and explosives (AA&E) and sensitive/critical assets. This guide also provides a synoptic review of DOD policy statements for key and lock control.

14. SUBJECT TERMS
Locks, keys, access cards, hardware requirements, AA&E, lock and key control, security

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	
Unclassified	Unclassified	Unclassified	UL

EXECUTIVE SUMMARY

This user's guide provides information and procedures that will aid in the distribution and control of mechanical and electronic keys. An effective access control (lock and key or electronic) program will help minimize the possibility of unauthorized access to a facility and/or assets in a facility. Possession of keys and access control cards represent primary authorization for an individual to enter a facility or have access to a particular asset. Possession of keys and access control cards by unauthorized individuals severely affects security and neutralizes the primary purpose of an access control program.

This user's guide presents information on establishing a program for protecting Department of Defense (DoD) assets against covert or insider threats. This guide is divided into five chapters and seven appendices that describe a process for controlling locks, keys and access cards or credentials. Chapter 2 describes DoD requirements for access control. Chapter 3 provides a structured program for controlling locks, keys and access control cards. Chapter 4 provides descriptions of software and hardware that are commercially available for controlling locks and keys. Chapter 5 provides a structured program that specifically addresses the control of locks and keys that protect critical assets. The appendices include a glossary of lock, key, and access control terms, references, a listing of manufacturers that offer software and hardware for access control, and forms that can be used to implement a comprehensive lock, key, or access card control program. The appendices also include a checklist for lock and key control, a sample lock and key control plan, and a general description of electronic access control systems.

CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

CHAPTER 1

INTRODUCTION

OBJECTIVE

The objective of this user's guide is to provide information and procedures that will aid in the distribution and control of mechanical and electronic keys. An effective access control (lock and key or electronic) program will help minimize the possibility of unauthorized access to a facility and/or assets in a facility. Possession of keys and access control cards represent primary authorization for an individual to enter a facility or have access to a particular asset. Possession of keys and access control cards by unauthorized individuals severely affects security and neutralizes the primary purpose of an access control program.

SCOPE

This user's guide presents information on establishing a program for protecting Department of Defense (DoD) assets against covert or insider threats. Subjects that will be covered include:

- References to DoD requirements for lock and key control
- Procedures for establishing a lock and key control program
- Procedures for establishing an electronic access card control program
- Key control software and equipment for implementing an effective lock and key control program
- Special lock and key control requirements for critical assets, such as arms, ammunition, and explosives (AA&E) and chemical and special weapons (C&SW)

BACKGROUND

Access control is a process for ensuring that only authorized personnel are allowed into a designated area. For covert threats, a person who is not authorized to be in the facility could attempt to enter using false credentials or bypass methods. For insider threats, employees with legitimate access to a facility could attempt to compromise an asset. The insider may or may not have legitimate access to the asset.

The assumed goal of an unauthorized outsider is to compromise an asset without being noticed. The purpose of access control is to keep unauthorized intruders from entering areas where they are not allowed. For the insider compromise, an access control program will limit access to assets within controlled areas to authorized personnel only. Regardless of whether the equipment used to limit access is mechanical or electronic, control of the device (locks, keys and access cards) that allows authorized entry into a secure area is vitally important to ensure that integrity of the system is maintained.

Levels of Protection

Four levels of protection can be applied to covert and insider threats. The levels of protection and their associated access control strategies are as follows:

- **Low-Level Protection.** This level requires a single access control element, such as a keyed lock, a combination-operated (mechanical or electronic keypad) lock, or an electronic entry control device, such as a card reader. Each of these elements admits any bearer with the authorized credential (key, card, or combination) to the controlled space.

- **Medium-Level Protection.** This level requires two access control elements. The two access control elements should identify the individual and authorize entry into the facility. Two primary approaches to access control exist. The electronic entry control option consists of a card reader and a keypad, onto which a personal identification number (PIN) can be entered. A key and electronic keypad for PIN entry is another alternative. A guard or receptionist can also be used to verify identification visually, based on identification credentials, in addition to one of the access control elements described for low-level protection. Access should be monitored at a central processing unit for this level of protection. Challenging procedures to prevent tailgating should also be required at this level.

- **High-Level Protection.** This level requires three access control elements. Biometric identification devices provide the third access control element, in addition to the two required for medium-level protection. Access must be monitored at a central processing unit at this level of protection. Challenging procedures or single pass equipment, such as sensors or optical turnstiles, to prevent tailgating must also be used at this level.

- **Very High-Level Protection.** This level requires three access control elements, as described for high-level protection. Access must be monitored at a central processing unit at this level of protection. In addition, anti-passback and tailgating prevention in the form of mantraps and full-height turnstiles must be used to ensure compliance with access control requirements.

Protection of Critical Assets

For the protection of critical assets, such as AA&E, C&SW, and highly pilferable items, forced entry becomes a major factor in the design of an access control system. Conventional electronic access control systems, using magnetic locks or electric strikes, do not provide adequate forced entry protection for these applications. Mechanical locking devices should be used where forced entry is a primary consideration. For these applications, strict key control becomes the only method for ensuring security and access control of restricted areas.

APPROACH

The approach used in this user's guide is to describe a program that addresses identified threats and describes software and hardware that can be used to implement a program that will effectively control locks and keys or access cards. Possession of keys and access control cards or credentials by an employee represent authorization given by the command to have access to a facility or area within the facility. In the control of access, the key and access cards provide similar functions in that they represent the same authority to enter and must be protected against loss or compromise.

Both mechanical and electronic access control systems have advantages and disadvantages in the control of access. Keys and access cards are different in terms of the level of sophistication required for duplication. Keys can be mechanically duplicated while access cards must be electronically read and duplicated. Both however are vulnerable to theft. Access cards have the advantage of requiring secondary credentials such as personal identification numbers or biometric verification that is not possible with mechanical key systems. On the other hand, mechanical keys that have a high level of resistance to picking and bypassing can provide a higher level of physical protection against entry attack than electronic systems that rely on solenoid actuated or magnetic locks.

The user's guide is divided into five chapters and seven appendices that describe a process for controlling locks, keys and access cards or credentials. Chapter 2 describes DoD requirements for access control. Chapter 3 provides a structured program for controlling locks, keys and access control cards. Chapter 4 provides descriptions of software and hardware that are commercially available for controlling locks and keys. Chapter 5 provides a structured program that specifically addresses the control of locks and keys that protect critical assets. The appendices include a glossary of lock, key, and access control terms, references, a listing of manufacturers that offer software and hardware for access control, and forms that can be used to implement a comprehensive lock, key, or access card control program. The appendices also include a checklist for lock and key control, a sample lock and key control plan, and a general description of electronic access control systems.

CHAPTER 2

DOD LOCK AND KEY CONTROL REQUIREMENTS

INTRODUCTION

All branches of the military service have established requirements for lock and key control to protect critical assets. References 1 through 11 in Appendix B provide specific requirements for the protection of arms, ammunition, and explosives (AA&E) and chemical and special weapons (C&SW), as well as general requirements for access control of restricted areas and critical assets.

Requirements for the physical security of sensitive AA&E (Risk Categories I through IV), including lock and key control, are covered in References 1, 2, and 5. C&SW requirements are covered in References 4, 10, and 11. References 1 and 11 apply to the:

- Office of the Secretary of Defense
- Military departments (Army, Navy, Air Force and Marine Corps)
- Chairman of the Joint Chiefs of Staff and Joint Staff
- Unified and specified commands
- Inspector General of the Department of Defense
- Defense agencies
- DoD field activities

References 2, 3, and 4 apply specifically to Navy activities. References 5, 6, and 10 apply specifically to Army and Air Force activities. References 7 and 8 apply specifically to Air Force activities.

REQUIREMENTS

Effective lock and key control programs are required for the protection of critical assets and restricted areas. Comprehensive lock and key control programs are mandatory for the protection of specific critical assets, such as sensitive AA&E and C&SW.

CHAPTER 3

ESTABLISHING A PROGRAM FOR CONTROLLING LOCKS, KEYS, OR ACCESS CREDENTIALS

INTRODUCTION

The primary purpose of a lock and key or access credential control system is to control access to lock cores and keys or to access control credentials that permit access to a particular building or structure.

Key and access control systems can be simple or complex, depending upon user requirements. As a minimum, lock and key or access control systems require a key or credential inventory, issue records, and a procedure for returning the key or access control credential once the user no longer needs it. When control of keys or access control credentials is abandoned or lost, re-establishing security can be time-consuming and expensive, especially for conventional lock and key systems.

It is the responsibility of the individual command to develop and implement a policy for controlling locks, keys and access credentials. An example of a typical instruction for general security and critical assets is shown in Appendix C. For general security, lock, key and access control is usually a part of a comprehensive security and loss prevention plan. For critical assets such as arms, ammunition and explosives (AA&E), control requirements are mandated by specific instructions (see Chapter 2).

This chapter is divided into two sections. The first section deals with mechanical locks and keys used for access control, and the second deals with electronic systems that use credentials, credential readers, and electronic locks for access control. See Appendix D for a description of typical electronic access control systems.

MECHANICAL LOCKS AND KEYS

Personnel and Duties

Commands should assign responsibility for the lock and key control program to a specific individual or group and define duties in writing.

Key Control Officer. The Key Control Officer (KCO) is responsible for the operation and general function of the command lock and key control program. The KCO typically reports to the commander or vice commander of the facility on all matters related to the lock and key control program. Specific duties should include:

- Determining the location and category of all locks at a facility
- Determining the status of all keys currently in use
- Arranging key storage, including selecting containers, key rings, key tags, etc.
- Ensuring that all key storage containers are used properly and in accordance with directives and instructions

- Identifying restricted or critical areas
- Recommending areas for enclave security and master keying
- Designating Key Custodians
- Establishing lock and core rotation schedules
- Establishing locations for code storage and, as available, computer program acquisition for lock and key code control
- Identifying qualified locksmith(s) for use by command
- Developing log procedures and forms for daily use
- Ensuring that lock and key procedures are known throughout the command through educational programs

If lock and key systems protect critical assets or controlled areas, the individual assigned the duties of a KCO should have a security clearance equivalent to the classification of the material or area being protected. Commands usually find it expedient to assign KCO duties to the command Security Manager/Officer because there are close ties to emergency services and command and control operations.

Key Custodian. The Key Custodian reports directly to the KCO for direction and implementation of the command's lock and key control program. Duties include:

- Conducting a quarterly inventory of custodial and sub-custodial key accounts
- Maintaining key control logbooks or computer records
- Meeting periodically with all Key Sub-Custodians to review key logs or records, discuss rotation schedules, disseminate command educational program information, and resolve lock and key control problems
- Assisting with the implementation of command policy on lock and key control
- Covering all other assignments relating to lock and key control, as designated by the KCO

The Key Custodian designated by the KCO should have a security clearance equivalent to the classification of the material or area being protected.

Key Sub-Custodians. Key Sub-Custodians are selected by a command subdivision or tenant command and approved by the KCO. The Key Sub-Custodian is assigned control of one or more keys, depending on requirements. For example, the fire department may be designated as a Key Sub-Custodian and may have access to all keys at a particular command. Subdivisions of the command may be sub-custodians when the subdivision requires different key applications than the rest of the command. Sub-Custodians should have a security clearance equivalent to the classification of the material or area being protected.

The Key Sub-Custodian reports directly to the Key Custodian for:

- All assigned keys, including master keys or change keys if required
- Proper logging of change keys
- Verification of key usage

- Monthly key inventories
- Attendance at monthly meetings with the Key Custodian
- Other assigned tasks relating to lock and key control at the command subdivision level

Locksmith. A locksmith can help develop a workable key control program. Locksmiths are sometimes in a position to see the day-to-day operations from a working level and can help identify and implement workable procedures. At large commands, the locksmith shop is sometimes a division within the security department. This arrangement makes it easier to:

- Provide direct assistance to users without additional organizational layers
- Initiate timely lockout investigations and emergency access
- Implement lock and key rotation programs
- Provide security training to the command

If a locksmith is part of a key control program, some considerations should include:

- Equipment. Modern locksmithing equipment, such as key cutting and core-assembly equipment, will increase productivity and improve quality. Computers can make the locksmith's work easier through the use of key code, key control, and master-keying programs that can improve accuracy, increase productivity, and reduce the possibility of compromised lock and key codes. Computers can also be used for precision and automatic key cutting. A clean and well-lit workspace with adequate room will aid in the precision work required of a locksmith.

- Education. A command locksmith should be adequately trained on the latest DoD policy and industry lock and key practices. Education can benefit the command through increased productivity, improved quality, and a broader range of service capabilities. Attendance at conferences, seminars, and classes should be included in the budget.

- Staffing. Staffing requirements depend on the daily schedule of re-keying, emergency access calls, lockouts, and lock rotation requirements. Adequate staffing will help ensure successful program execution. Commands may want to consider assigning swing or graveyard shifts for locksmiths to allow more time for administrative work, re-coring, and rotation efforts without the pressures of emergency calls, daytime work distractions, and disruption of the daytime workforce.

  Contracting with a civilian locksmith service can increase the productivity of a small staff and improve emergency response. Civilian locksmith services should be bonded and have security clearances as required by DoD and local policy. The contract agreement for civilian locksmith services needs to contain requirements for adherence to all command lock and key control policies and procedures.

Key Control Training

A program should be developed to train command personnel in lock and key control procedures and responsibilities. Training should be comprehensive and provide a strategic

understanding of how lock and key control can affect the security of a command. Training should include the following topics:

- How to minimize the risk of a lock compromise
- Lock maintenance requirements
- Lock and key control procedures
- What to do in case of a lockout
- Proper key security, including procedures for dealing with lost, missing, stolen, or damaged keys

Training programs should be designed to hold the attention of attendees. Use examples and scenarios that describe real situations and problems (e.g., thefts that have taken place or careless acts that can compromise a key control program). Diagrams, videos, pictures, or charts can be used to illustrate the subject and make the training more interesting. Regardless of the method, constant training of command personnel is essential to a successful lock and key control program.

Facility Evaluation

Before initiating a lock and key control program, the KCO, the Key Custodian, and the Key Sub-Custodians should survey all lock locations throughout the facility with emphasis on:

- Priority of assets protected
- Requirements for access to the assets
- Lock/core rotation and re-keying schedules
- Enclaving and master-keying requirements
- Status of lock and key control training
- Schedules for periodic meetings to make reevaluations
- Requirements by tenant commands or command subdivisions for lock and key support
- Established agency requirements and policies (see Chapter 2)

Procedures

Key Control Centers (KCC). At large commands, a KCC should be established where daily key issue and recording activities take place. If possible, co-locate the KCC with a 24-hour staffed site, such as an emergency services or dispatch center. The KCC should have adequate personnel cleared at the appropriate classification level to provide lock and key control services. The key issue point should be located where it will not interfere with normal operations. The Watch Officer during each shift should account for all controlled keys and maintain a chain-of-custody log. Activities at the KCC should include:

- Key Issue. The KCC should control access to any key other than a personally assigned change key. Personnel requiring the use of a key should be designated in a Key Access Log (for descriptions of logs see Records Management in this chapter and Appendix E). The Key Access Log should be accessible only to KCC duty personnel. Separate key

control logs should be used for issues and returns. Compare the signature on the Key Control Log with the signature on the Key Access Log.

Bring any deviations from normal patterns to the attention of the KCO. Under normal circumstances a master, restricted, or sensitive material control key should not leave the facility or remain with any person during the day or overnight.

- Key-Making. Duplicate keys, key blanks, padlocks, lock cylinders and cores, key-making equipment, and key codes should be stored in a Central Key Room. Access should be limited to the base Commander, KCO, Key Custodian, and locksmith. The Central Key Room must always be secured when not in use. Key blanks and duplicate keys have the same classification and require the same protection as original keys. At commands too small to justify a Central Key Room, a General Services Administration (GSA)-approved security container can be used to protect duplicate keys, blanks, key codes, and associated equipment.

- Key and Core Code Storage. Maintain codes for keys and lock cylinders or cores in the Central Key Room. Keep these codes in an approved security container with access limited to the KCO and locksmith. Treat code information in the same manner as classified documents. Do not allow unauthorized viewing or copying of these documents.

Master-Keying. The term "master-keying" is used to describe a method of pinning a specific set of lock cylinders so they operate with an individual key as well as a common key, called a "master." A "set" of master-keyed cylinders could be as small as two locks or as large as several thousand. Large master-key systems usually offer numerous levels to allow flexibility and security.

Professionally designed and maintained master-key systems can be very effective at saving time and money. Such systems are tailored to the objectives and operation of the organization. Systems can be set up so each major component of the organization is covered by a segment of the overall system. This allows the designer to "build-in" room for expansion or area re-keying, without affecting the rest of the system.

Effective master-key systems minimize the number of keys each employee needs to gain access to authorized spaces and equipment. Issuing low-level master keys gives the security officer the ability to limit the number of keys issued and also allows access to only those locks the employee needs to open. Higher level master keys need to be strictly controlled and should only be issued if absolutely necessary.

Key control is critical to a successful master-key system. If a top-level master key is lost or stolen, the entire facility may need to be re-keyed. This is expensive and time consuming. If a low-level master key is lost or stolen, only the locks that operated with that key would need to be re-keyed.

Although master-key systems are proven to save time and money, they should not be used in all cases. Security officers need to be involved in the design and decision processes. Master-keying is primarily used in unclassified administrative spaces. High security locks and locks used to protect classified or high value assets should never be master-keyed.

Personnel designated to establish and/or maintain a master-key system need to be trained and qualified to perform that function. Master-key and key control training courses are available through professional locksmith organizations.

Examples of keying are shown in Figures 3-1 and 3-2. Figure 3-1 shows a system that allows a number of locks to be operated with the same change key. There is no limit on the number or type of locks that can be keyed alike. Figure 3-2 shows a master-keyed system, where each lock has its own individual key (change key) that will not open any other lock, and a master key that will open all locks. For more information on the subject of master-keying, see Reference 12.

Key Indexing and Marking. Indexing systems simplify tracking keys and cores. A single identification system consists of a simple record of key identification symbols, corresponding to a lock location and a record of key issues. Identification aids include a ledger, record book, card index or other recording device, and key tags. A multiple identification system is used when specific control of keys is required to conceal the identity of lock applications and/or locks.

A typical indexing system will start with the broadest area affected by that key, then take it to an individual lock. For example, the index 301-244-A could mean Building 301, Room 244, Desk A. This system makes it easy for program personnel to match keys and locks. It also might make it easy for someone who finds the key to determine where the lock is located, and this should be considered a vulnerability.

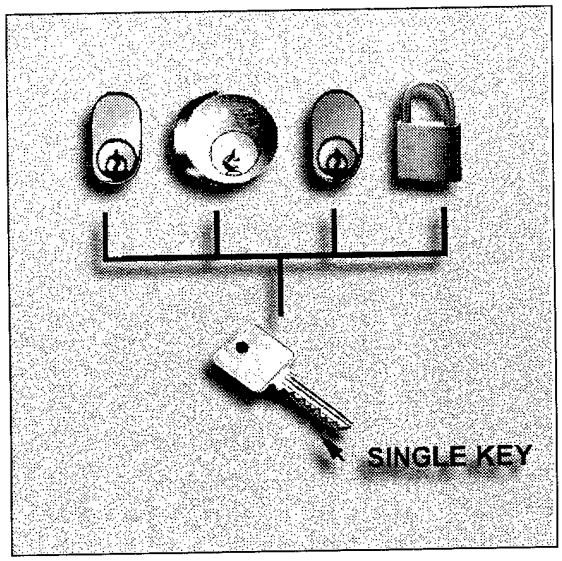


Figure 3-1. Keyed-Alike System

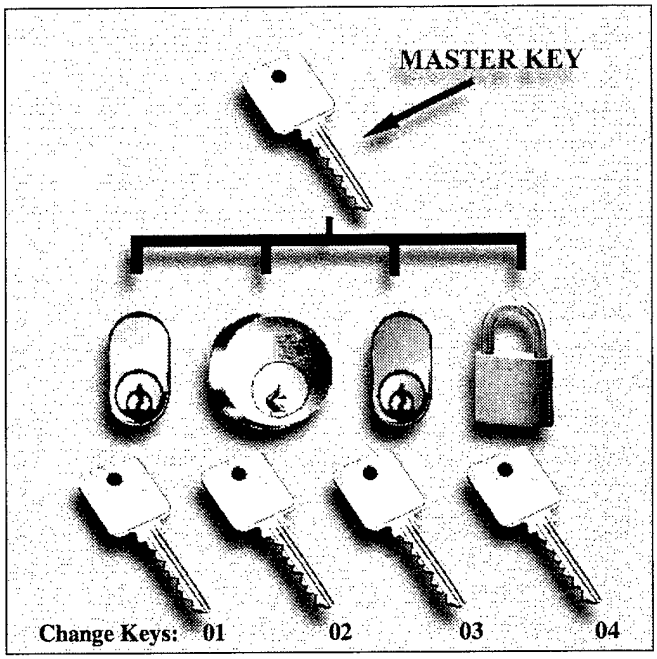
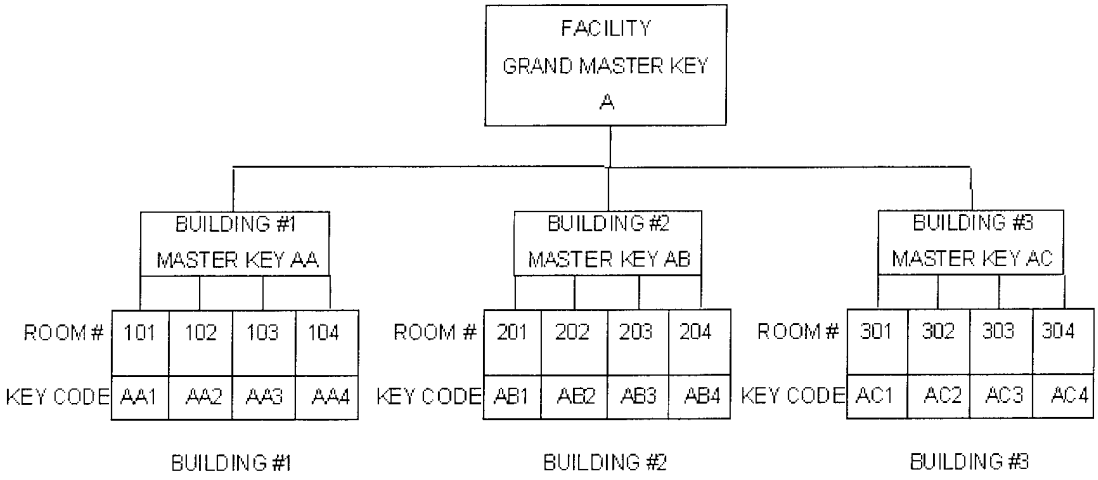


Figure 3-2. Master-Keyed System

A sample facility master-keyed system is shown in Figure 3-3.



Key Code	Level*	Operates
A	GMK	All
AA	MK	All AA (Bldg. 1)
AA1	CK	Room 101
AA2	CK	Room 102
AA3	CK	Room 103
AA4	CK	Room 104
AB	MK	All AB (Bldg. 2)
AB1	CK	Room 201
AB2	CK	Room 202
AB3	CK	Room 203
AB4	CK	Room 204
AC	MK	All AC (Bldg. 3)
AC1	CK	Room 301
AC2	CK	Room 302
AC3	CK	Room 303
AC4	CK	Room 304

*CK = Change Key, MK = Master Key, GMK = Grand Master Key

Figure 3-3. Sample Door Schedule

A more complex indexing system is used when greater control of keys is required. This system might use random or sequential numbers on keys. The index numbers are recorded in the Key Inventory Log along with the core or cylinder numbers. The tightly controlled Key Inventory Log then becomes the only source of information matching a key with a core or cylinder.

Index code numbers, as well as an index of all locks and keys, should always be secured. These records are typically kept in a GSA-approved security container in the Central Key Room.

For ease of locating the proper key, key tags may be marked with explicit locations and the index number stamped on the key. The tag should not be issued to the user.

Records Management. Lock and key control software, as well as paper-based systems, are available for record management.

- Paper-Based System. Traditional lock and key control record management systems use handwritten documents. Logs and forms can be customized by individual commands for their specific use. Appendix E contains examples of logs that provide the required information. Bound logs are recommended to reduce the possibility of record tampering. Accurate documentation is critical in maintaining the physical security of an installation. Most paper-based systems include the following:

  1. The Key Inventory Log (Table E-1 in Appendix E) tracks keys, lock cylinders and includes:
     - The key index code and corresponding lock core/cylinder index code(s)
     - The location(s) of the locks opened by that key

  2. The Key Access Log (Table E-2 in Appendix E) tracks personnel who have access to keys and includes:
     - Name and department code
     - Office and home phone numbers
     - Employee/military ID number
     - Signature (for purposes of comparison)

  3. The Key Control Log (Table E-3 in Appendix E) tracks key usage and includes:
     - The date and time a key is issued
     - The serial numbers and total number of keys issued
     - The person receiving the issued key
     - The person issuing the key
     - The time and date when key is returned
     - The person receiving the returned key

  4. The Key Issue Record (Table E-4 in Appendix E) provides an audit trail for key assignment and includes:
     - Name
     - Employee/Military ID number
     - Number of keys issued

- Applicable building number, floor, room number, container, cage, section or area
- Statement of responsibility (see Table E-4 for description of statement)

5. The Key Manufacturing Request (Table E-5 in Appendix E) provides an audit trail for making keys and includes:
   - Requester
   - Number of keys required
   - Justification for the request
   - Location of the lock
   - Authorization for the request

6. The Lock Repair/Service Request (Table E-6 in Appendix E) provides an audit trail for repairing and servicing locks and includes:
   - Requester
   - Location of the lock
   - Description of the problem
   - Resolution of the problem

- Lock and Key Control Software. Paper-based key control systems are time consuming and expensive. Lock and key control software is available that can track keys and users and produce reports, such as total keys in the system, users, locations, and check-out/check-in data, etc. Programs are also available to assist with core/lock rotation and maintenance, pinning codes, cylinder/core locations, and key-bitting codes and data. A more complete description of commercially available software developed specifically for lock and key control is included in Chapter 4.

Equipment. A wide variety of equipment is commercially available for storing and tagging keys. For a description of these items, see Chapter 4.

Emergency-Use Keys. Emergency access to all buildings and gates is a requirement for life safety. Delay in access to a facility or area could greatly increase damage or endanger occupants or emergency service personnel. For this reason, consider designating fire and security departments as facility Key Sub-Custodians. Co-locating fire and security dispatch services (including the KCC) at the fire department could eliminate the need for issuing duplicate master keys to both emergency services.

In those instances where security becomes the overriding consideration, commands may choose to have emergency services gain entry by force. This can be difficult, dangerous, and time consuming, particularly when high-security systems are in place. In a security situation, forced entry by the response force may jeopardize the lives of emergency personnel or building occupants. One solution is an emergency lock box mounted outside a building (Figure 3-4). It will securely hold the keys to the building and can be opened only by emergency personnel.

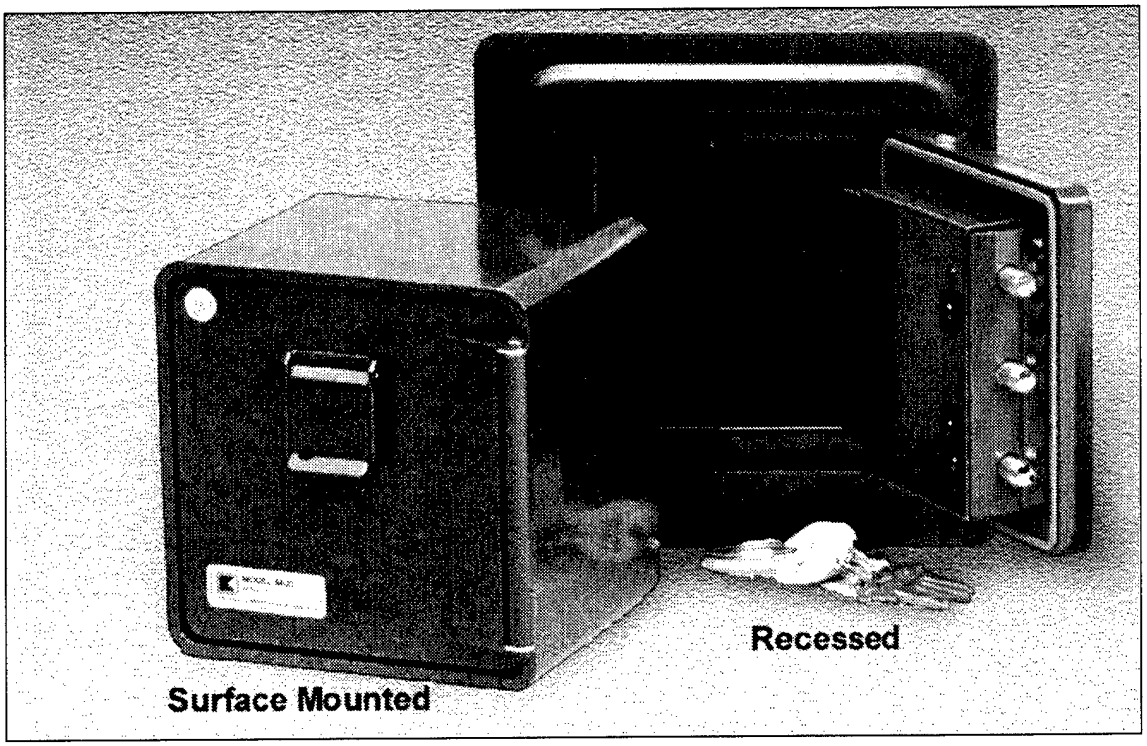


Figure 3-4. Emergency Key Box

Lockout Procedures. Mechanical locks will sometimes fail or keys break inside the keyway making the lock unusable. Lockouts must be reported to the KCO and investigated for possible tampering.

Effective lock and key control programs include established procedures for entrance into a perimeter, building, office, or container affected by a lockout. Procedures should include provisions for entry without destroying the damaged lock, to preserve it for later examination.

If it is impossible to determine the cause of the lockout from initial inspection, or if the cylinder/core cannot be removed, a locksmith should remove the lock with the approval of the KCO. Once the lock has been removed, the Key Custodian should verify that all personnel entering the area are authorized. Any forced entry should be documented and witnessed by two or more people. Provisions should be made to immediately secure the area.

Lockouts normally require re-keying, re-coring, or replacement of the lock. Evidence of lock tampering also requires re-keying, re-coring, or replacement and investigation by security personnel.

Supply Centers. The large number of locks needed for supply centers usually requires enclaving and master keying. Areas highly subject to pilfering should be considered for rotation at least three times annually. Areas or facilities where access could be compromised by employee turnover should consider supplemental methods of securing those areas, including use of antipilferage seals.

Personnel Termination. Cylinders should be re-keyed or locks re-cored when personnel are terminated. This is particularly important if the personnel had access to restricted areas.

Key Disposal. Used or obsolete keys should be controlled until properly destroyed. Keys should be destroyed in such a way that they cannot be used or copied. Using a metal grinder to remove the key bitting is an effective method.

Lock Maintenance

Maintenance plays an important role in the operation of any lock. All locks and cylinders/cores should have a routine maintenance schedule. Locks exposed to natural elements or harsh environments should receive more frequent maintenance.

A lock has many small parts. Lubrication is an important maintenance item to ensure the locks will continue to work properly. Some fluid lubricants use a petroleum-based carrier that tends to hold dirt in the lock components, adversely affecting tolerances and causing premature lock failure. Extremely low or high temperatures can make a lubricant gel freeze or thin, causing the lock to fail or produce extreme wear that will lead to eventual failure. Always follow the manufacturer's recommendations for maintenance and lubrication of locks.

Funding

Funding for lock and key control programs typically comes from the command operation and maintenance funds. Lock rotation programs must be balanced against available funding, but lack of funding should not restrict the program to the point where security is compromised. Assistance from the facility comptroller is helpful when planning a lock and key control program.

Documentation

Document all lock and key control program procedures. Maintain written instructions for every aspect of the program to make procedure standardization easier. Ensure that all program personnel are assigned duties in writing.

ELECTRONIC ACCESS CONTROL SYSTEMS

Personnel and Duties

Identify the personnel involved in the access control program and define their duties. Avoid verbal orders; all personnel duties must be in writing. Efficient use of personnel can make a significant difference in the effectiveness of an access control program.

Access Control Officer (ACO). The ACO should be responsible for the operation and general function of the access control program. The ACO typically reports to the commander or vice commander on all matters related to organizing the access control program. Specific duties include:

- Determining the location and category of all access-controlled doors
- Determining the status of all access credentials currently issued
- Identifying areas of higher security requiring secondary credentials
- Recommending areas for possible enclave security
- Recommending credential reissue and recoding schedules
- Recommending locations for central processing and monitoring units
- Ensuring that access control procedures are known throughout the command through educational programs
- Covering all other assignments relating to access control, as designated by the facility commander

The ACO should have a security clearance equivalent to the classification of the material or area being protected. The Security Officer/Manager is often selected as the ACO because of the close ties to emergency services and command and control operations.

Access Control Training

Develop programs to train personnel in access control program procedures and responsibilities. The training should be comprehensive enough to provide a strategic understanding of how access control can affect the security of a command. Provide regular training on topics such as:

- How access control systems work
- How to prevent defeat of access control systems
- How access control computer systems and software operate
- Maintenance methods
- Access control procedures
- Procedures for handling rejected credentials
- Proper access control security, including what to do if a credential is lost, missing, stolen, or damaged

Training programs should be designed to hold the attention of attendees. Use examples and scenarios that describe real situations and problems (e.g., thefts that have taken place or careless acts that can compromise a key control program). Diagrams, videos, pictures, or charts can be used to illustrate the subject and make the training more interesting. Regardless of the method, constant training is essential to a successful access control program.

Facility Evaluation

Prior to starting an access control program, the ACO should make a survey of all access control locations throughout the facility with emphasis on:

- Priority of assets protected
- Requirements for access to the assets
- Access control credential reissue schedules
- Enclaving requirements
- Status of access control training
- Schedules for periodic meetings to re-evaluate requirements
- Requirements by tenant commands or command subdivisions for access control support

Procedures

Access Control Centers. For large commands with extensive electronic access control requirements, it may be necessary to establish an Access Control Center where the daily access control credential issuing and recording activities can take place. If possible, these centers should be co-located with 24-hour staffed sites, such as emergency services dispatch centers. They should have adequate personnel to provide access control services. The access control credential issue point should be located where it will not interfere with emergency personnel, such as dispatchers or operators.

Blank access control credentials should be stored in a GSA-approved security container with access limited to the ACO and an alternate. Treat blank access control credentials in the same manner as classified documents. Do not allow unauthorized access to blank credentials.

Records Management. Electronic access control systems normally include software programs that allow the tracking and management of access control credentials. The data base may contain information regarding badge authorization and can include badge number, employee number, name, address, telephone, motor vehicle registration, status, issue date, return date, authorization center, portal restrictions by time zones, entry/exit status, and trace. A commentary section may also be included that is used for emergency call lists and other safety-related information. Computers containing personal and classified data of this nature should be secured at all times.

Lockout Procedures. When an electronic access control component (credential reader, electric strike, or magnetic lock) fails or a credential denies access to the user, the incident must be reported to the ACO.

An effective access control program should have established procedures for entrance into a building or office when the access control system fails. Any forced entry or bypassing of the

electric lock should be documented and witnessed by two or more people. The ACO should make provisions to immediately secure the area. Access control system failure at the access portal normally requires repair or replacement of the electric lock, strike, and/or reader.

Personnel Termination. Access codes should be immediately removed or canceled when personnel are terminated. This is particularly important if the personnel had access to restricted areas.

Access Control Credential Disposal. Used or obsolete access control credentials should be controlled until properly destroyed, especially if they are also used as identification badges. Credentials should be destroyed in such a way that they cannot be used or copied. Using a crosscut shredder is a good method for destroying credentials.

Maintenance

Maintenance of credential readers is normally not required, other than periodic cleaning of the credential swipe path (not required for proximity sensors). Electric strikes require routine periodic maintenance and lubrication, similar to mechanical locking devices. Magnetic locks require little maintenance. Credential readers and electric strikes exposed to natural elements or harsh environments should receive more frequent maintenance.

Funding

Funding for access control programs typically comes from the command operation and maintenance fund. Software and data base maintenance should be balanced against available funding, but lack of funding must not restrict a program to the point where security is compromised. Costs for periodic updates on access control software should be included in the budget. Assistance from the facility comptroller is important when planning an effective access control program.

Documentation

Document all access control program procedures. Maintain written instructions for every aspect of the program to make procedure standardization easier. Ensure that all program personnel are assigned duties in writing.

CHAPTER 4

KEY CONTROL SOFTWARE AND EQUIPMENT

INTRODUCTION

This chapter contains a representative listing and description of locks, software and related equipment that can be used to establish an effective lock and key control program. A listing of manufacturers and suppliers of this type of equipment and/or software is in Appendix F. ***This is not a complete list and any reference to a manufacturer is included only to illustrate a piece of equipment or software. It is not intended to be a recommendation or an endorsement of any product or company.***

KEY CONTROL SOFTWARE AND HARDWARE

Paper-based key control systems can be very time-consuming. Reports other than what is contained on a single record sheet will require a significant amount of time to generate.

Computer-based programs track keys and users and produce reports, such as total keys in the system, users, locations, and check-out/check-in data. Other programs are available to assist in core/lock rotation and maintenance, pinning/key bitting codes, and cylinder/core locations. Still others can interface with electronic locking systems to activate and deactivate locks remotely and provide specific access control for spaces and key storage.

Computerized record-keeping programs can store, arrange, search, and analyze data or automatically produce reports based on the data. These programs typically have built-in report forms that can be customized by the user and search features to isolate and arrange input data into specialized formats. Special applications for use by AA&E facilities or supply centers are also available. These programs can list keys by location hook numbers, as well as by lock locations. Additional programs link key-cutting machines directly to computers for cutting keys.

Tables 4-1 and 4-2 provide a brief description of commercially available hardware and software that supports lock and key control programs.

Table 4-1. Examples of Commercial Key Control Hardware Systems

Product	Features
KeyTrak (Figure 4-1)	• Drawers are electronically locked • Keys are released by magnetic card and/or password • Optical scanners detect any changes in a drawer when the drawer is opened or closed • Alarm sounds if a key is taken by an unauthorized person
The KeyWatcher by Morse (Figure 4-2)	• All key movements are tracked by time • Individual user codes are used to increase security • Card reader interface compatibility • On-demand audit trail reports • Alarm outputs, tamper, overdue, etc. • Access limited by time zone and day of week • Can be operated by modem • Can be used as either a stand-alone or an integrated system • Real-time transaction reports • Battery backup
KEYSURE (Figure 4-3)	• Key control for individual keys, access control cards, computer passwords, alarm codes, safe combinations, encryption codes, etc. (tamper-evident sealed plastic container) • Prevents duplication or surreptitious use of stored material • Protects stored material and provides physical accountability for access
InstaKey (Figure 4-4)	• Convenient user re-keying • Security and control of keys through the manufacturer • Low cost master-keying • Software available for control of all keying records • Retrofit capabilities to existing locks • Manufacturer's support and training
TracAccess by Supra (Figure 4-5)	• Electronic keypad similar to a calculator • Can be configured many ways to give access to different people, at different times, and keep a complete record of access activity • Information can be transmitted to the keypad directly from a PC or remotely via modem • Operates a family of electronic locks and key storage systems available from the manufacturer
Key Systems Key Monitor (Figure 4-6)	• Key movement in or out of locked monitor cabinet automatically recorded by time, date, and user code • Keys can be timed and alarmed to ensure return • Tamper-alarmed cabinet with PIN entry • Audit trail of last 4,800 events • Battery backup

Table 4-2. Examples of Commercial Software for Lock and Key Control

Product	Features
KRM by LockSoft	• For a multiple key system, tracks: Keys Key issue Key return Re-keying Key inventory
Key-Z by Morse	• Tracks: Which key opens which lock Number of keys for each lock in the inventory Keys that have been reported missing, lost, stolen, recovered, or destroyed Number of keys issued and to whom
Key Trail by HPC	• On-screen key control maintenance • Issues keys individually or in a group • Handles interchangeable core systems • Tracks: Keys held Locations Personnel Lost keys Overdue keys Work orders for keys • Password protected • Interfaces with other HPC software for master-keying and code retrieval

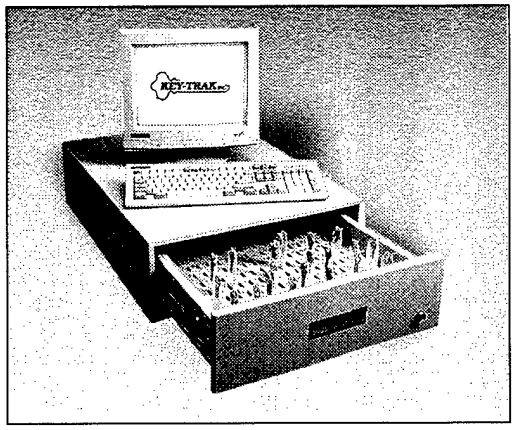


Figure 4-1. KeyTrak

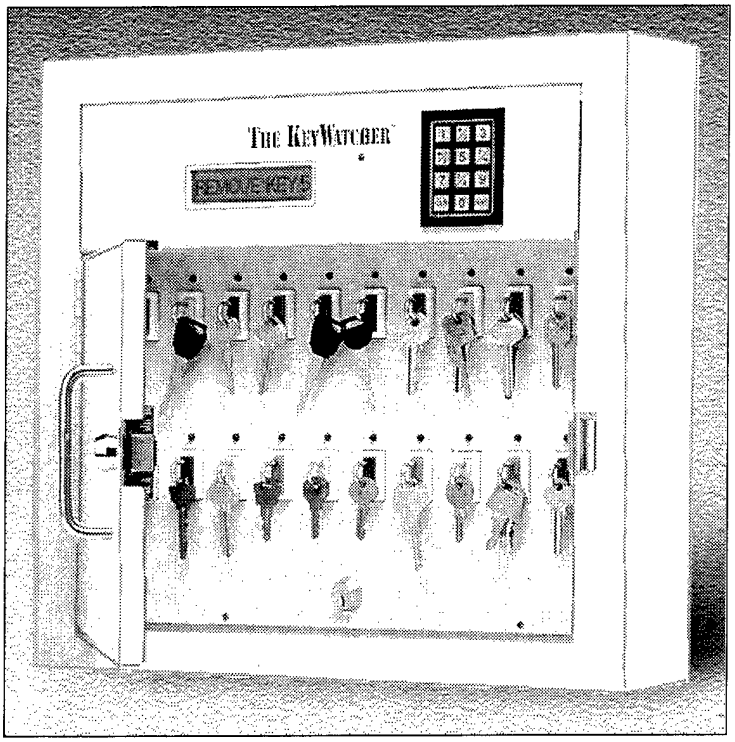


Figure 4-2. The KeyWatcher

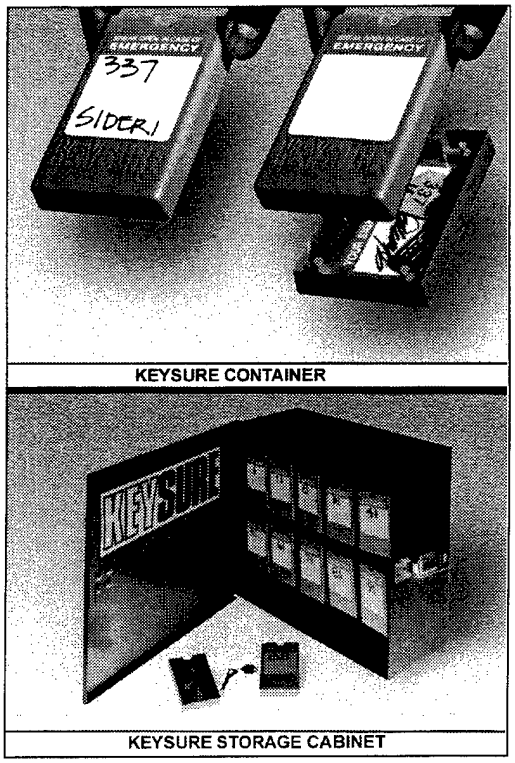


Figure 4-3. KEYSURE

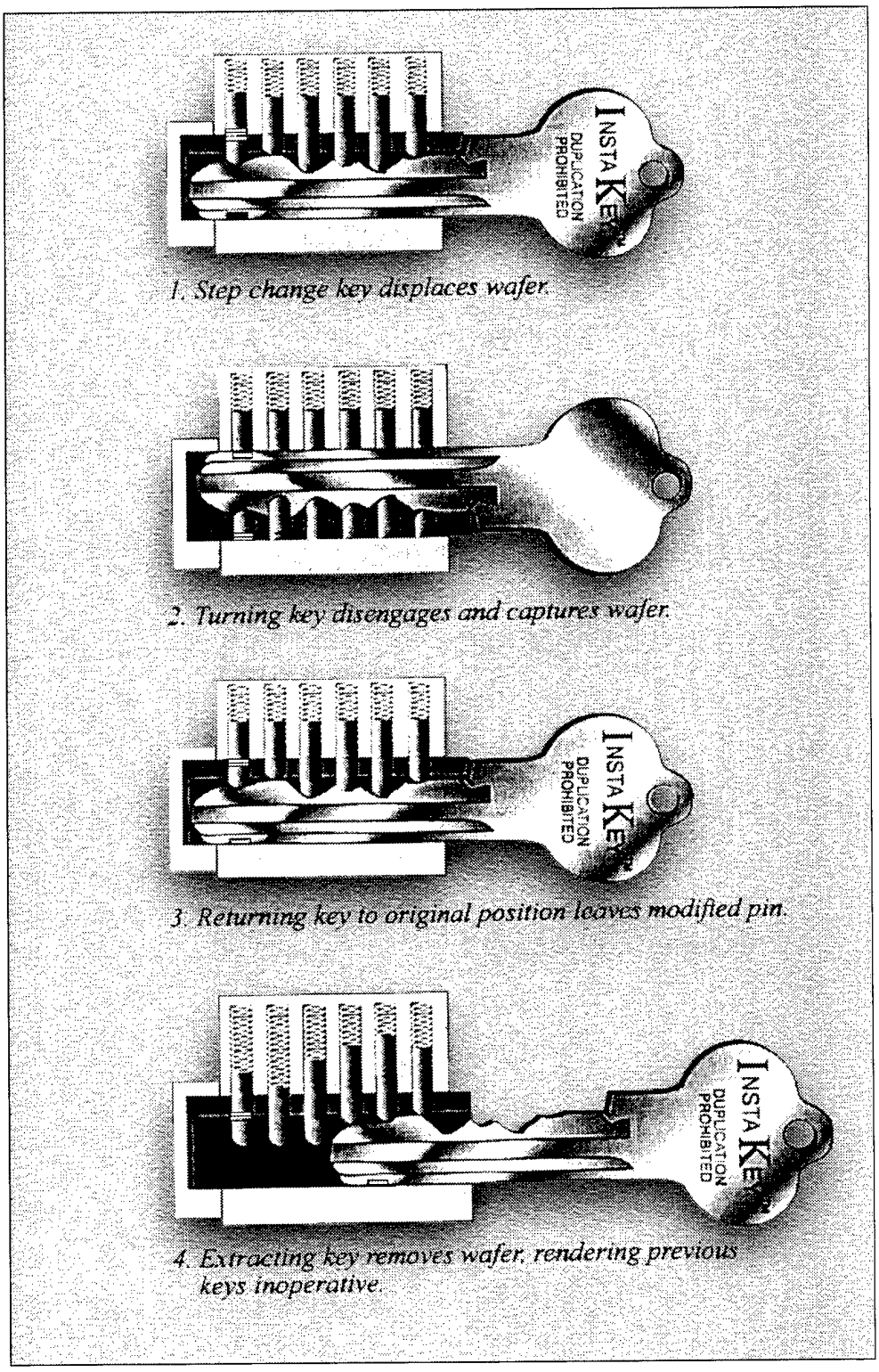


Figure 4-4. InstaKey

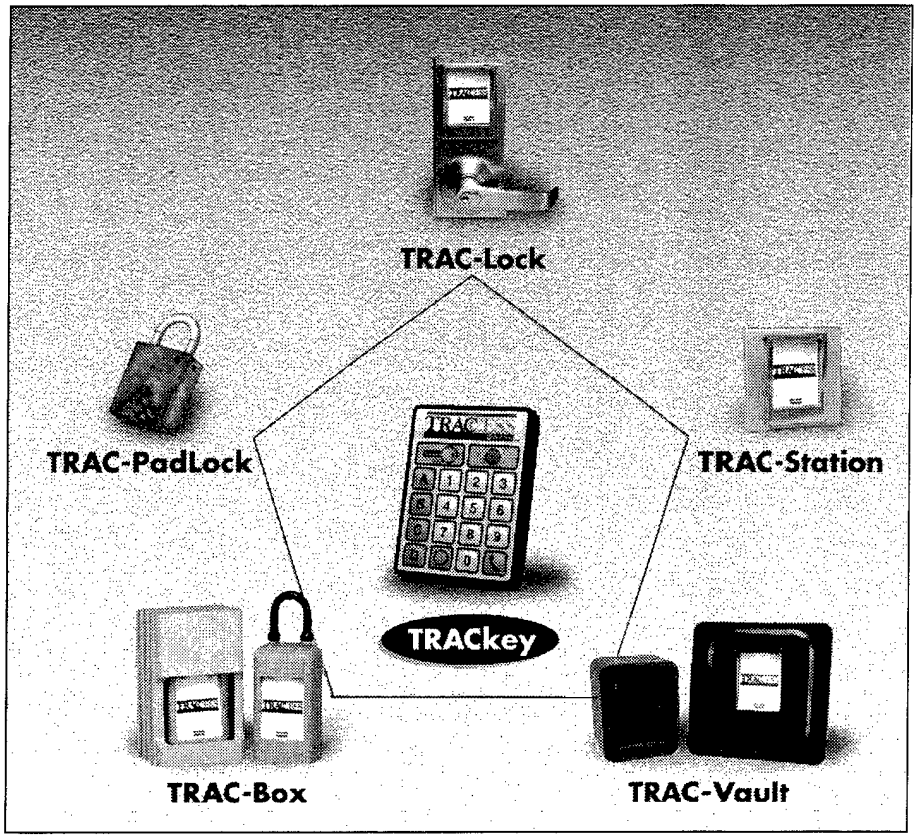


Figure 4-5. TracAccess System

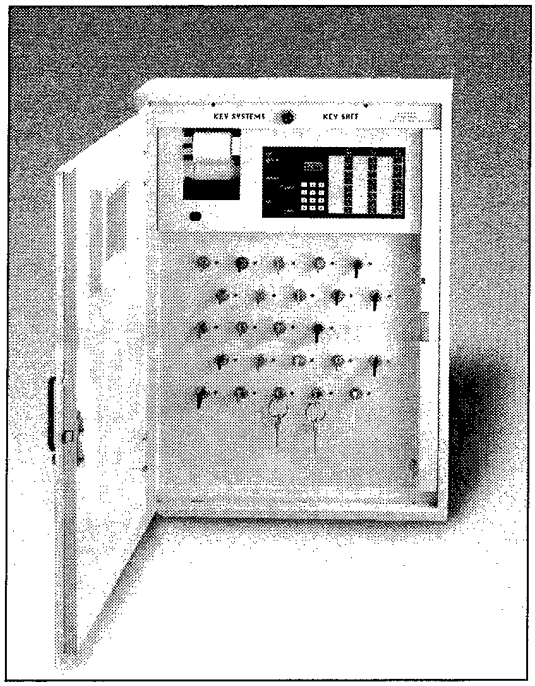


Figure 4-6. Key Systems Key Monitor

MECHANICAL LOCK AND KEY SYSTEMS

Low-Security Locks and Cores

Low-Security Padlocks. The low-security padlocks shown in Figure 4-7 are just a few of the many different types and styles that are available. Both General Services Administration (GSA) and the Defense Supply Center Philadelphia (DSCP) purchase and stock low-security padlocks. These locks are key-operated, pin tumbler with five or six pins, and can be purchased to be keyed alike, keyed individually, or mastered (Table 4-3). Low-security padlocks can be purchased from DSCP against Commercial Item Description (CID) A-A-1927 (Table 4-4).

Low-security padlocks can be used to deter unauthorized entry. They provide limited resistance to forced entry and only minimal resistance to surreptitious entry. Low-security padlocks listed in Tables 4-3 and 4-4 have a dead bolt that locks the "heel" of the shackle that is retained in the lock body and the "toe" of the shackle that is released. They also retain the key in the cylinder when the padlock is in the unlocked condition and the shackle is hardened against a physical attack using small bolt cutters.

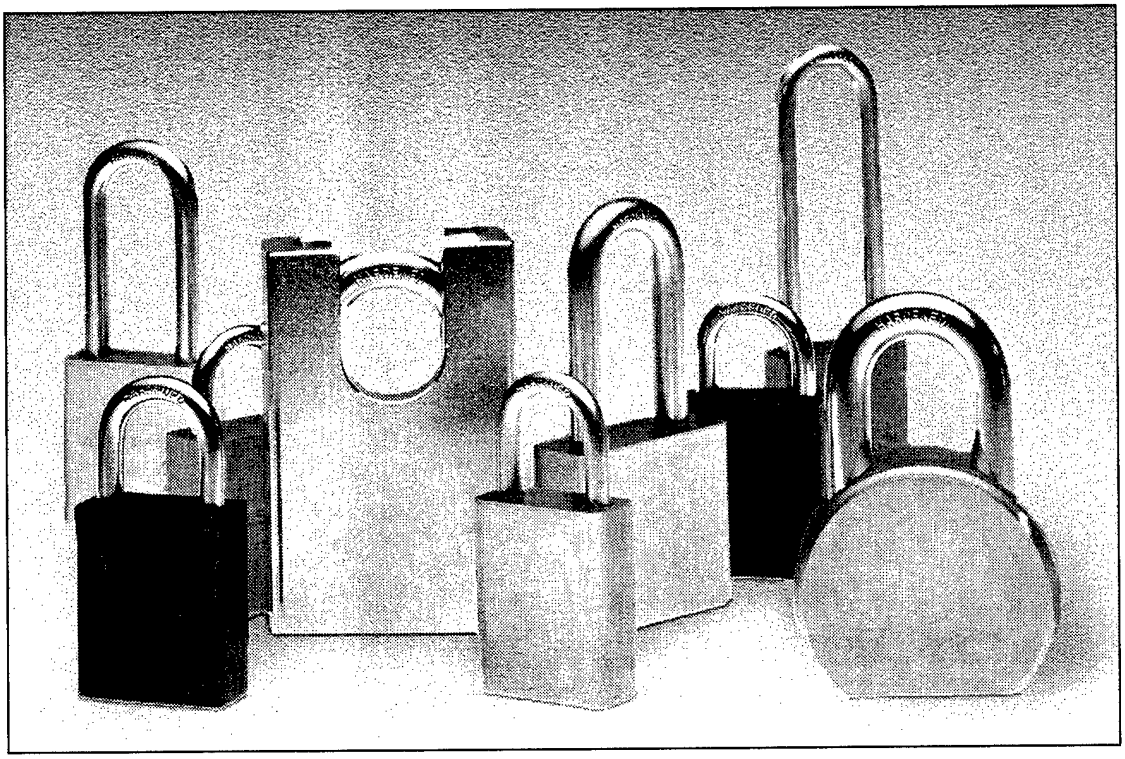


Figure 4-7. Low-Security Padlocks

Table 4-3. Low-Security Padlocks Available through GSA

National Stock Number	Nomenclature
5340-01-346-4611	Padlock, steel body and 3/8-inch hardened shackle: Conforming to ASTM F833, Type PO1, Grade 2
5340-01-346-4612	Padlock, steel body and 3/8-inch hardened shackle: Conforming to ASTM F833, Type PO1, Grade 2 (with chain)
5340-01-346-7462	Padlock, brass or bronze body and 3/8-inch hardened steel shackle: Conforming to ASTM F833, Type PO1, Grade 2
5340-00-285-6523	Combination Padlock: Conforming to Federal Specification FF-P-110 (with a 3/8-inch hardened steel shackle)

Table 4-4. Low-Security Padlocks Available through DSCP

National Stock Number	Nomenclature
5340-00-158-3807	Padlock: (With chain) steel case and 3/8-inch hardened steel shackle
5340-01-408-8434	Padlock: Steel case and shackle with a 3/8-inch diameter, 3-1/2-inch long hardened steel shackle
5340-01-269-9345	Padlock: Brass body with a 3/8-inch diameter, 2-1/2-inch hardened steel shackle
5340-01-408-8452	Padlock: (With chain) steel case and 3/8-inch hardened steel shackle - 10 Locks per set
5340-01-437-0625	Padlock: (With chain) steel case and 3/8-inch hardened steel shackle - 6 Locks per set
5340-01-437-0627	Padlock: (With chain) steel case and 3/8-inch hardened steel shackle - 24 Locks per set

General Field Service Padlock (GFSP). The GFSP provides resistance to forced entry equal to the hardened chain or hasp it will be used with and high resistance to a variety of environmental conditions.

Federal Specification FF-P-2827, Padlock, General Field Service can be used to procure this padlock. The GFSP is available through the GSA Schedule and the Federal supply system in two sizes shown in Table 4-5.

The GFSP is an excellent choice for a wide variety of applications. This padlock is recommended where padlocks are exposed to dust, grit, corrosive environments, or freezing conditions.

Note: Hardware requirements for a specific application should always be verified by referencing the appropriate security instruction.

To order contact:

ABLOY SECURITY, INC.
GSA Contract Number GS07F0368J
6015 Commerce Drive
Suite 450
Irving, TX 75063

At (800) 367-4598 or (972) 753-1127 and ask for Customer Service.

Product	**Description**
PL655 – Meets FF-P-2827A	3/8" Diameter Shackle x 1-1/4" Clearance
PL101	Replacement Cylinder w/2 Keys
PL656 – Meets FF-P-2827B	1/2" Diameter Shackle x 1-1/2" Clearance
PL102	Replacement Cylinder w/2 Keys
Available Configurations	Sets Keyed Different, Keyed Alike, or Master-Keyed

ALL LOCKS AND CYLINDERS PRICED LESS KEYS

7104000522	Cut Keys with Locks
7104000522	Cut Keys without Locks
MSKY	Master Keying Charge (per Lock)

Minimum Order: $100.00

Table 4-5. General Field Service Padlocks Available through DSCP

National Stock Number	Nomenclature
5340-01-380-9430	Padlock, General Field Service w/3/8-inch shackle
5340-01-380-9432	Padlock, General Field Service w/1/2-inch shackle

Mortise Locks. A mortise lock is pictured in Figure 4-8. It is so named because the lock case is mortised or recessed into the edge of the door. The most common type has a doorknob or thumb latch on each side of the door. Either knob will operate the latch. This type of lock comes in a number of configurations that can be locked from the inside or outside by either a thumb turn or key, or from the edge of the door by a pushbutton or rocker switch, depending on the lock's construction and function. Mortise locks are used on building entrance doors, office doors, storage closets, etc., and are low-security locking devices.

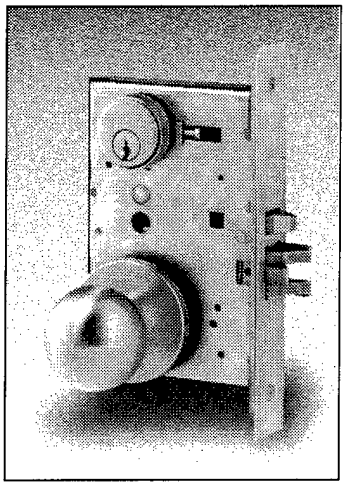


Figure 4-8. Mortise Lock

Cylindrical Locks. The cylindrical lock (Figure 4-9) is the most common of all door locks in use today. The key-in-lever lock is similar in construction to the key-in-knob lock, except for the lever action. This type of lock is used to secure office doors, storerooms, and exterior doors. It gets its name from the locking cylinder located in the knob or lever. Some cylindrical locks require a key to lock and unlock them. Others unlock with a key, but must be locked by pushing or rotating a button on the inside knob. All may be used with a deadlatch to keep the latch from being depressed by end pressure. These locks are strictly low-security devices.

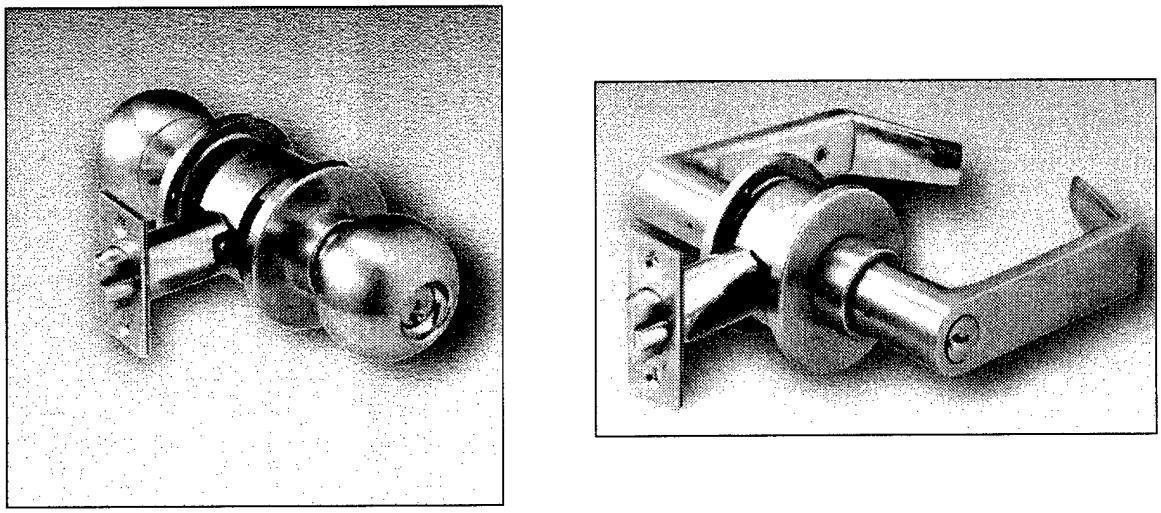


Figure 4-9. Typical Key-in-Knob and Key-in-Lever Lock

Deadbolt Locks. The deadbolt lock (Figure 4-10), also referred to as a tubular deadbolt, is similar to the cylindrical lock in that it is mounted in a hole cut through the door. When the bolt is extended, force applied to the end of a deadbolt lock will not retract it. The deadbolt, used in conjunction with a cylindrical lock, provides considerably greater security than a low-security padlock and hasp, if there is sufficient engagement of the bolt into the jamb (at least 1-inch). Single- and double-cylinder deadbolt locks are the two types most commonly used. A single-cylinder deadbolt has one cylinder facing the outside and is operated by a key. The inside is operated with a thumb turn. This type is more secure when used if there are no windows in the proximity of the lock. The second type is a double-cylinder lock that has a cylinder on both sides. This requires that a key be used to lock and unlock from either side of the door. This type of lock is best used when nearby windows will provide easy access to the lock. Caution should be used when selecting a double-cylinder lock to ensure that its use does not violate requirements for life safety.

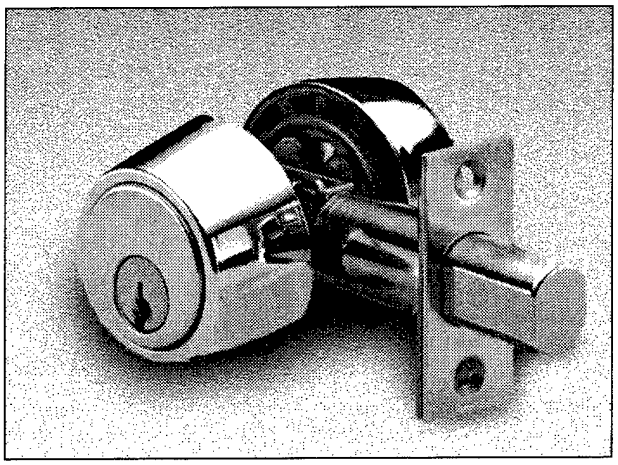


Figure 4-10. Double-Cylinder Deadbolt Lock

Interchangeable Core Systems

Interchangeable core systems can include deadbolts, key-in-knob locks, rim locks, mortise locks, padlocks, and desk and cabinet locks. All locks in an interchangeable core system can accept the same core. Some examples of interchangeable core locks are shown in Figure 4-11. The common feature of interchangeable core locks is a figure 8-shaped core that houses the tumblers and springs. The cores can be easily removed and replaced using a control key. An interchangeable core lock can be re-keyed by simply replacing the core.

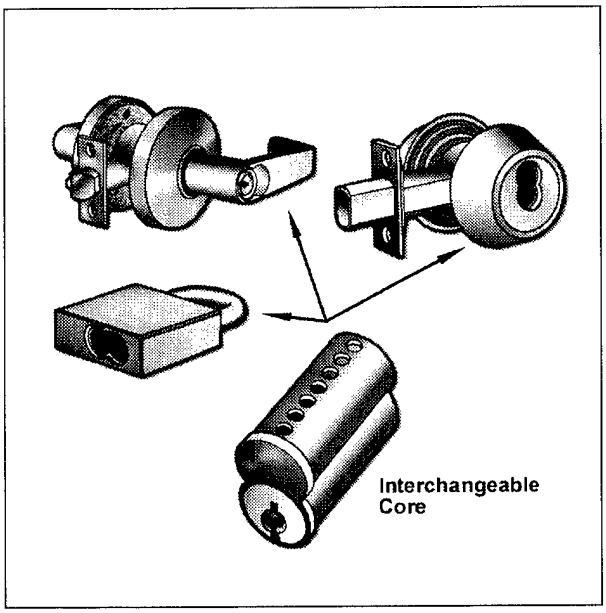


Figure 4-11. Interchangeable Core Locks

KEY STORAGE EQUIPMENT

General Key Storage

For key storage, use solidly constructed metal key storage containers. Wooden boards with nail or hook arrangements do not offer security for key storage. It is best not to use exposed key storage for any keys.

For supplemental control, store master or grand master keys in a separate key box sealed with an antipilferage seal. Seals, such as a car ball or wire seal as shown in Figure 4-12, or other types of seals, should be used to indicate tampering or entry. The key box can also be placed inside a GSA-approved security container.

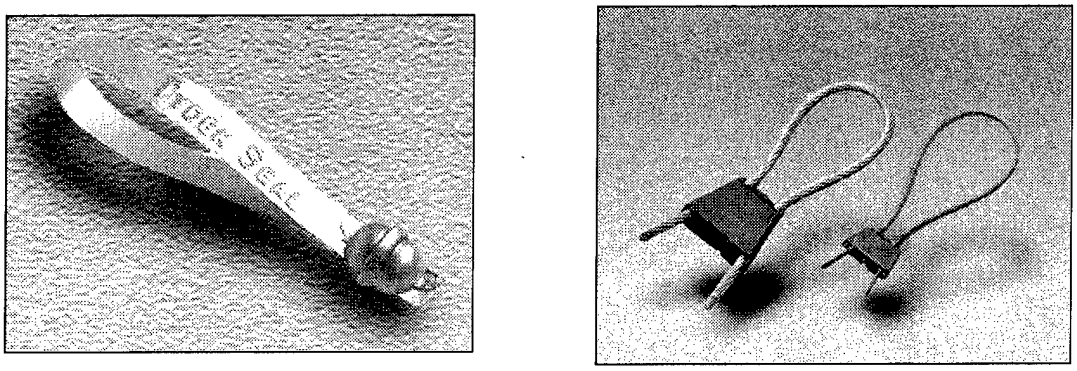


Figure 4-12. Examples of Antipilferage Seals

Log the serial number of the antipilferage seal into the duty-personnel-turnover log, especially if the seal is broken. The antipilferage seal must be part of an overall seal control program (refer to DoD "Antipilferage Seal User's Guide," Reference 9 in Appendix B). Limit key box access to the Commanding Officer, Key Control Officer, and/or assigned representative. Use lockable key storage containers for all routine applications in Key Control Centers. Secure key storage containers when not in use to avoid the possibility of compromise. Consult authorized access lists before issuing a key. Do not display access lists where unauthorized persons can see them.

In small commands, key control can be handled by the KCO/Key Custodian. Keys should be stored in a lockable key cabinet or GSA-approved security container. Access to this container should be limited to the KCO/Key Custodian or Commanding Officer.

Key Cabinets, Lockers, and Safes

Selecting the proper key control cabinet depends upon its intended use in the system. A wide variety of key cabinets are available, including wall-mounted (flush or recessed), table-mounted, multiple-drawer, and portable. The capacity of these cabinets ranges from about 20 keys for the smallest wall-mounted cabinet to over 3,300 keys for an 8-drawer cabinet.

Most standard key cabinets have the same type of lock as an office desk and provide approximately the same minimal protection. Although dual combination locks and padlock-locking systems are available for key cabinets, they do not increase the overall security protection provided by the cabinet. Key cabinets should not be used for the storage of keys to sensitive materials. Such keys are to be stored in security containers, as required by applicable security instructions.

Placement of the key cabinets within the facility is important. The cabinets should be located within a room or building that is either locked or attended at all times. Keys to the cabinets should also be controlled.

Key cabinets are available with single and multiple identification systems. A single identification system provides only the lock labels, temporary key tags, and permanent key tags. A multiple identification system is a complete, cross-indexed system of records for recording alphabetically the hook number, core number, core codes, and master-keying information. Complete key control systems include all necessary components, such as key-gathering envelopes, hook labels, temporary key tags, receipt holders, receipt forms, an index, and an instructional manual.

The cabinets may be purchased separately, in which case only the cabinet and hook labels are furnished. Accessories, such as tags and additional panels for expanding the capacity, may be purchased with or for the above systems.

Lockable, wall-mounted key cabinets with key hooks, key tags, and a single identification system are described in detail by CID A-A-2547 and are available in the Federal supply system.

In addition to key-lockable storage cabinets, key safes are also available from commercial sources. Key safes offer the most secure storage for keys. Master keys should be stored in this type of container if it is properly anchored to prevent removal. Key safes are not recommended for daily use because of the time required to gain entry. Some key safes are designed to fit in classified material containers for additional security.

Figures 4-13, 4-14, 4-15, and 4-16 show examples of key cabinets, safes, and lockers.

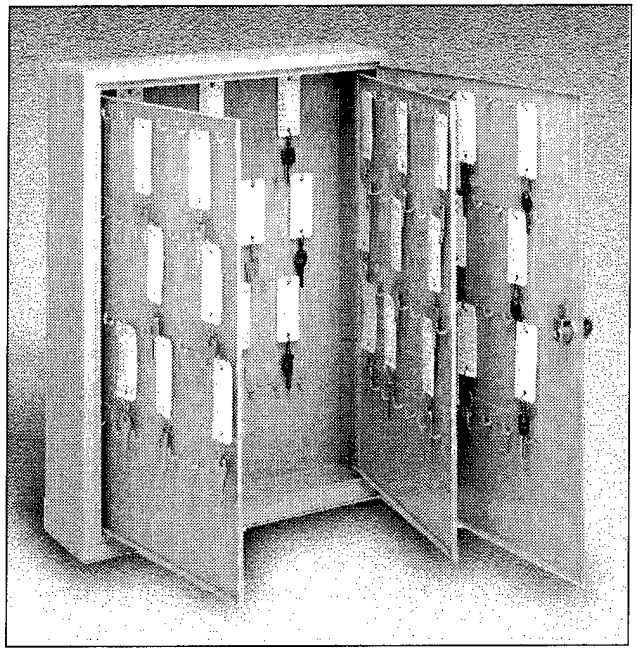


Figure 4-13. Key Cabinet

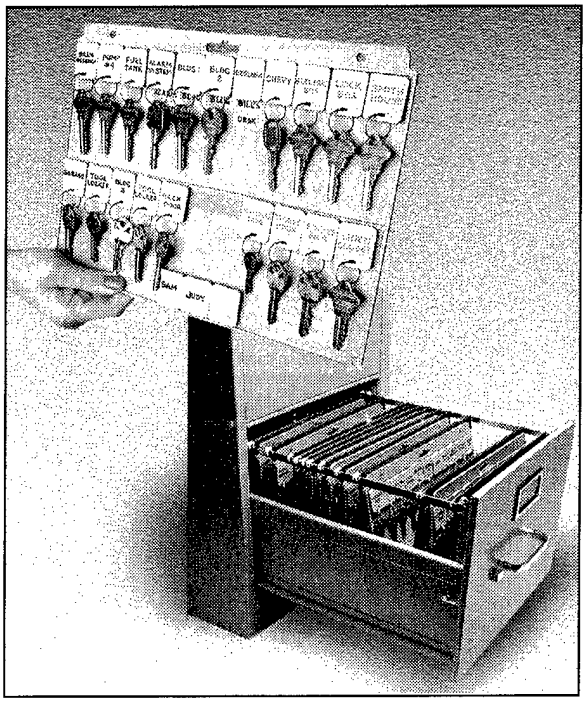


Figure 4-14. File Cabinet Insert

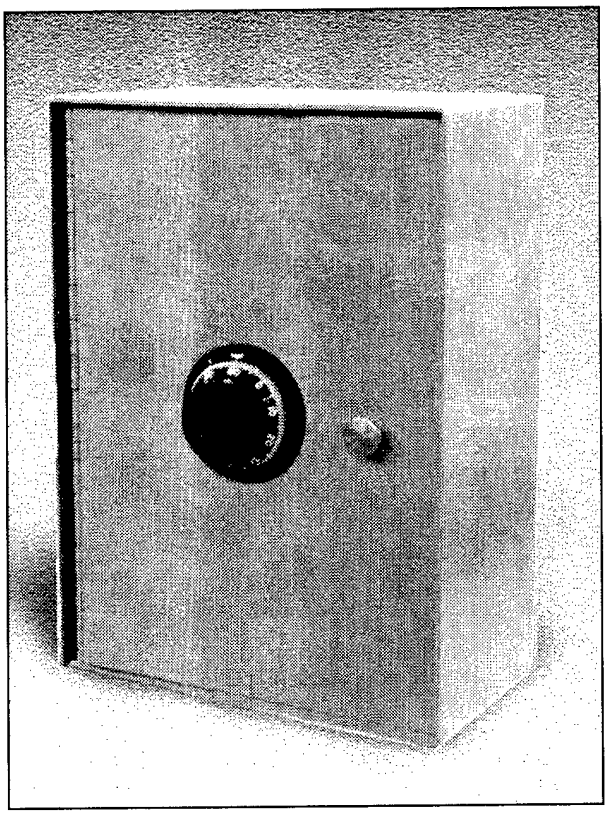


Figure 4-15. Key Safe

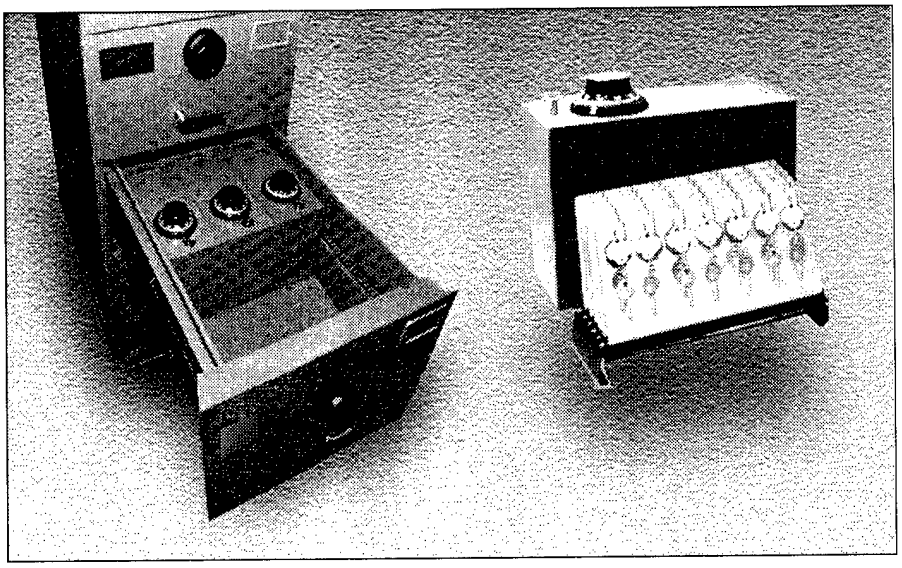


Figure 4-16. Utility Key Locker

Key Tags and Key Rings

A system of indexing and tagging keys is crucial to an effective lock and key control program. Choose key tags that are readily recognizable and easily readable. There are tags available through the Federal supply system (NSN 9905-00-245-7826) that meet the criteria. Tagging systems are also available from the commercial sources (see Figure 4-17).

Select key rings that are resistant to accidental openings. If your level of security warrants it, choose one-time rings that must be destroyed to remove the keys. These rings may also be coded with serial numbers and designed to show evidence of tampering. One-time rings are typically secured with a crimping tool. Figures 4-18 and 4-19 are examples of tamper-resistant key rings.

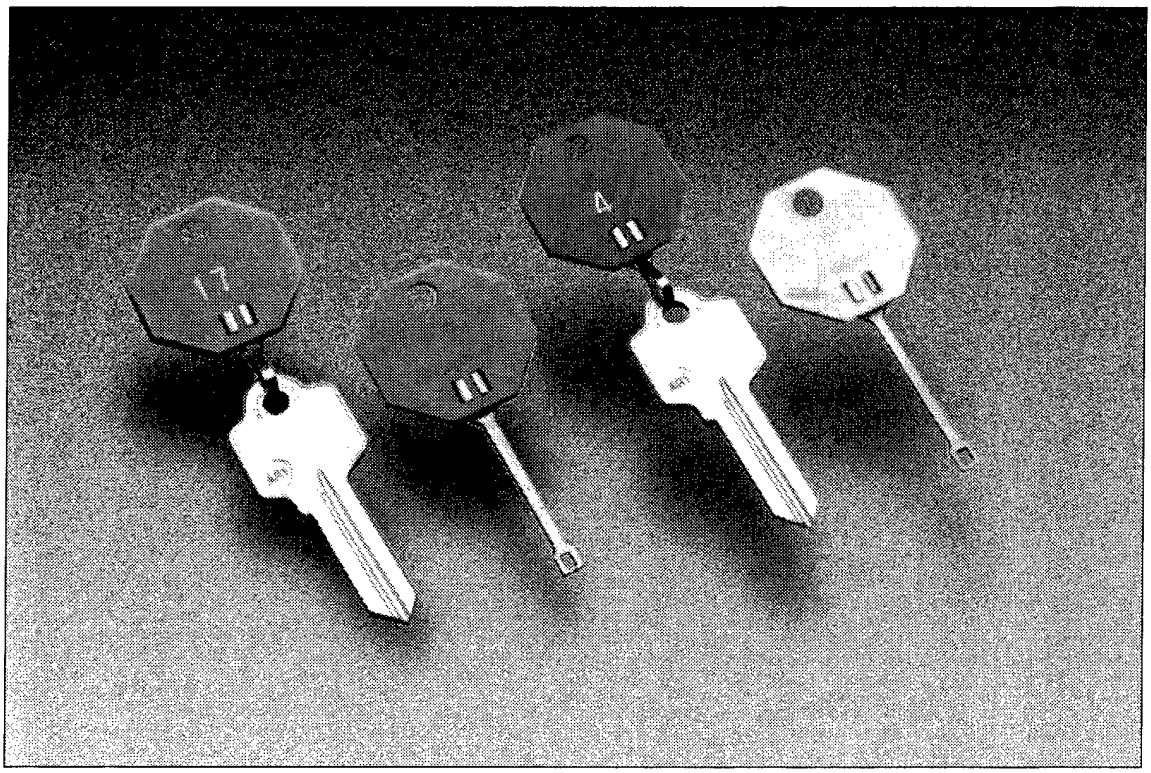


Figure 4-17. Key Tags

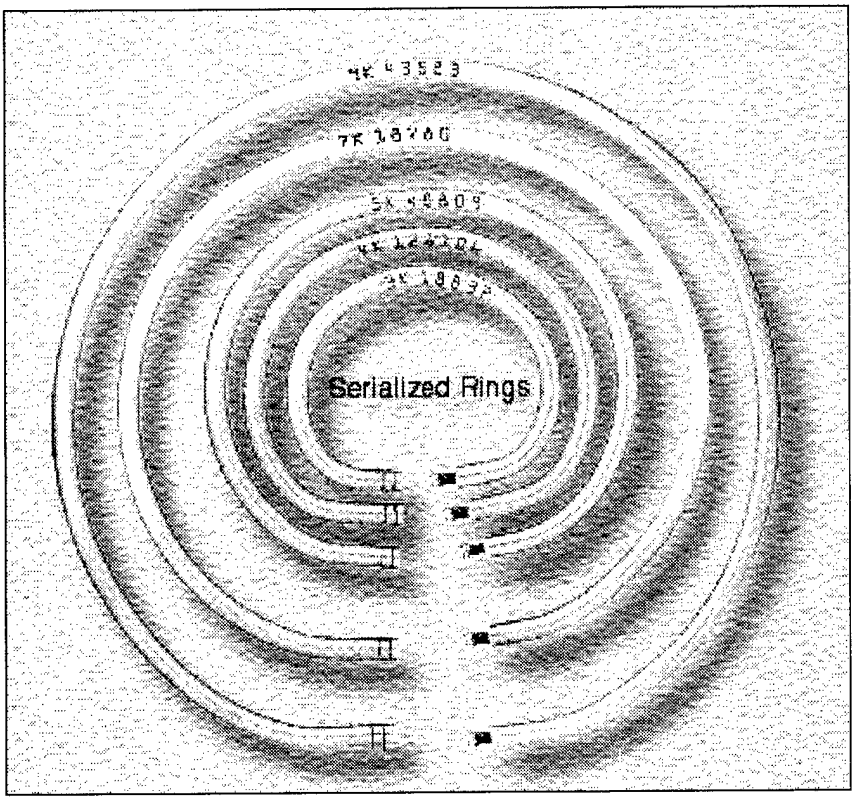


Figure 4-18. Key Rings

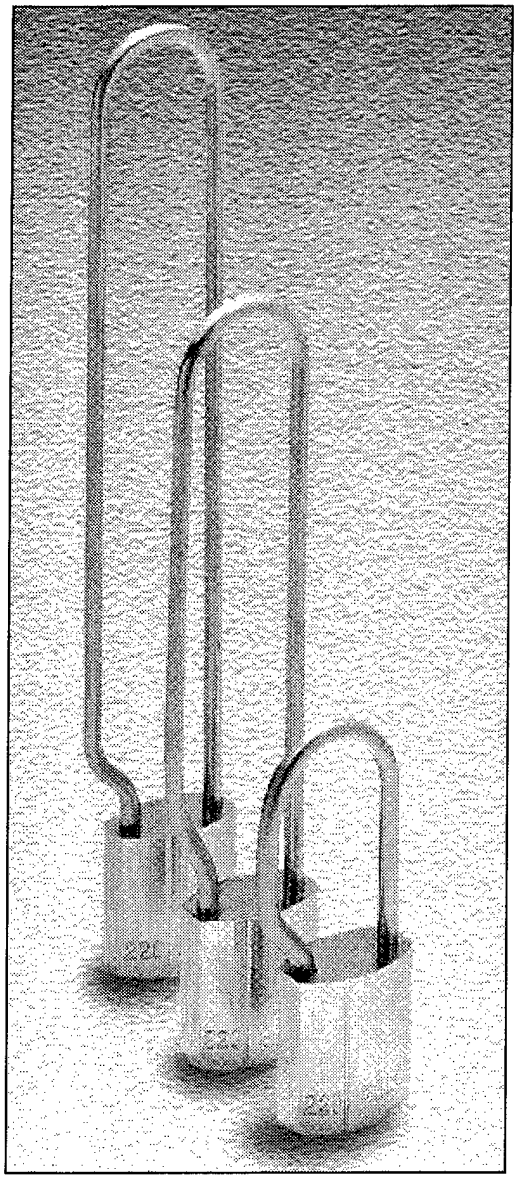


Figure 4-19. Padlock-Type Key Rings

CHAPTER 5

LOCK AND KEY CONTROL FOR CRITICAL ASSETS

INTRODUCTION

Protection of critical assets, such as AA&E, C&SW, sensitive material or equipment, and highly pilferable items, requires a structured and strict approach to key control. Protection of these assets is covered by References 1 through 11 in Appendix B.

SPECIFIC REQUIREMENTS

AA&E Facilities

1. Keys to areas protecting AA&E must be maintained separately from all other keys.
2. Keys should only be issued to personnel from authorized access lists.
3. Authorized access lists should not be available to unauthorized individuals.
4. The number of keys issued for any single lock should be held to a minimum.
5. Keys must never be left unattended.
6. Keys must never be left unsecured.
7. For Category III and IV AA&E, only designated key storage containers with at least 20-gauge steel construction, an Underwriters Laboratories (UL) 768-listed, built-in, Group 1 changeable combination lock or a GSA-approved combination padlock (Sargent and Greenleaf (S&G) Model 8077) shall be used.
8. Keys to Category I and II AA&E shall be stored in a Class 5 GSA-approved security container.
9. Keys must never leave the facility or remain with any one individual during operations or overnight.
10. High-security locks must be rotated or re-keyed at least annually or when keys are lost, misplaced, or stolen.
11. Replacement or reserve locks, cores, and keys shall be secured in designated key storage containers or a Class 5 GSA-approved container to prevent access by unauthorized individuals.
12. A lock on a storage facility must operate with only its own change key (no master keying or keying alike is allowed).
13. A lock and key custodian must be appointed and designated in writing.
14. A key control log must be maintained to ensure key accountability (Table E-3 in Appendix E).
15. Accountability records shall be retained for 90 days.
16. Padlocks shall be locked to the staple or hasp when the area or container is open.
17. Inventories of keys and locks shall be conducted semiannually.

18. Positive, two-person control is recommended for all Category I through IV magazine and storage entries, except in special cases, and then only in strict adherence to applicable requirements.

C&SW Facilities

Key control for C&SW facilities applies to storage structures, buildings, rooms, and containers in both limited and exclusion areas, as well as keys to intrusion detection systems, perimeter gates, and manhole covers. In addition to the lock and key control requirements for AA&E, the following must be implemented for special weapons and Category I, II, and III chemical weapons:

1. Keys to C&SW storage facilities shall be controlled as classified material and stored in a Class 5 security container.
2. Keys must be maintained separately from all other keys.
3. Keys and locks must be audited monthly.
4. Keys shall be inventoried with each change of custody.
5. Positive, two-person control is required for access to all C&SW storage facilities.
6. Two-key entry (two separate locking systems or one locking system with two keys) is mandatory to ensure compliance with the two-person requirement.

Sensitive and Highly Pilferable Material or Equipment

The following requirements apply:

1. Keys should never be left unattended.
2. Keys should never be left unsecured.
3. Commercial, lockable key storage containers should be used.
4. Open storage of keys that are accessible to unauthorized individuals should be avoided.
5. Keys should never leave the facility or routinely remain with any one individual during operations or overnight.
6. Access to keys should be made strictly from authorized access lists only.
7. Authorized access lists should not be displayed where unauthorized individuals can view them.

Designated Key Storage Containers

Containers designated for secure key storage (Table 5-1) must be made of 20-gauge steel or an equivalent-strength material (Figure 5-1). They must be equipped with a UL 768-listed, built-in, Group 1, changeable combination lock or modified to accept a GSA-approved, three-position, changeable combination padlock, S&G Model 8077, NSN 5340-00-285-6523 (Figure 5-2).

Table 5-1. Designated Key Cabinets

Cabinet	National Stock Number
Wall-mounted, one-door, with integral key lock, 75-key capacity	7125-00-132-8973
Wall-mounted, one-door, with integral key lock, 95-key capacity	7125-00-285-3049
Wall-mounted, one-door, with integral key lock, 190-key capacity	7125-00-285-3048
Wall-mounted, one-door, with integral key lock, 1,000-key capacity	7125-00-132-8981

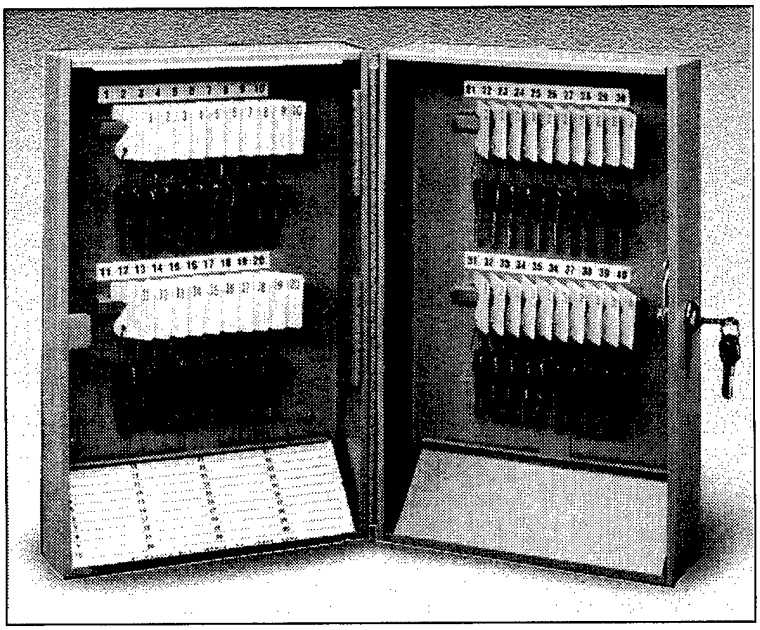


Figure 5-1. Key Cabinet

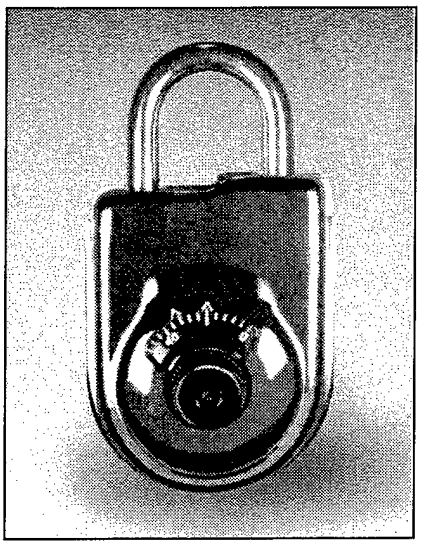


Figure 5-2. GSA-approved, Three-position, Changeable Combination Padlock (S&G Model 8077)

Lockouts

Lockouts at critical facilities present a unique security concern. If high-security locks are rendered inoperable and a lockout occurs, policy should include multilayered redundancy for verification. Policies should include verification by the KCO and Key Custodian/Key Sub-Custodian of any action used to gain entry (e.g., lock removal, hasp removal, hinge removal). Any high-security device requiring forced entry should be completely investigated to verify whether the lock has been tampered with or failed because of a malfunction. **For information on how to proceed with an investigation of a lock that has malfunctioned for an unknown reason, contact the DoD Lock Program Technical Support Hotline at the Naval Facilities Engineering Service Center (NFESC), Port Hueneme, CA, (805) 982-1212 or DSN 551-1212.**

If forced entry is required, the contents of the secured area must be protected by armed guard or be properly secured prior to departure of the repair party. Magazines with intrusion detection system (IDS) sensors rendered inoperable must receive 24-hour armed guard protection until the IDS sensors can be repaired.

High-Security Lock Hardware

The following requirements apply:

- Entry doors to armories and magazines storing AA&E or C&SW must be secured with a high-security locking system (Table 5-2). Interior doorways may use GSA-approved Class 5 vault doors, equipped with a UL 768-listed, Group 1 combination lock.

- Facilities where aircraft or vehicles are stored with weapons on board must be secured with a high-security locking system, or equivalent compensatory measures.

- Doors not normally used for entry must be secured from the inside with locking bars, deadbolts, or padlocks. Bolt-type seals or cable-type seals could also be used for this purpose. Panic hardware, when required, must be installed to prevent opening the door by drilling a hole and/or fishing from the outside. Panic hardware must meet life safety, fire, and building codes and be UL-listed or, when applicable, meet host country requirements.

- Padlocks must be locked to the staple or hasp when a door or container is open to preclude theft, loss, or substitution of the lock.

- For the Navy, Marine Corps and Coast Guard, the Naval Surface Warfare Center (NSWC), Crane Division, Crane, Indiana, issues, repairs, and replaces cylinders and locks, and issues keys for S&G 833C high-security padlocks. Damaged or malfunctioning locks and requests for cylinder and key replacement will be sent by registered mail to Commanding Officer, Naval Surface Warfare Center Crane Division, 300 Highway 361, Crane IN 47522-5060 [Code 7095] (telephone 812-854-1354 or 3354; DSN 482-1354 or 3354; FAX: 812-854-1074). Non-Navy customers interested in these services can call NSWC to discuss specific requirements and payment options.

- Locks and/or lock cores should be rotated annually for security purposes.

- A preventive maintenance (PM) program must be established and operated for all high-security locking systems. All high-security locks should receive PM once a year and more often if subjected to severe environmental conditions (dust, sand, salt air, extreme cold, etc.).

- The NFESC is the DoD Locks, Safes, Vaults, Seals, and Containers Program Technical Manager. Questions about any of these items may be directed to the DoD Lock Program Technical Support Hotline 1-800-290-7607, commercial phone 805-982-1212, DSN 551-1212, E-mail dodlock@nfesc.navy.mil or Web Site HTTP://locks.nfesc.navy.mil .

Table 5-2. High-Security Locking Systems for Protection of Critical Assets

APPROVED LOCKS*		
National Stock Number	**Description**	**Notes**
5340-01-217-5068	Padlock, key-operated, high-security, shrouded shackle (Figure 5-3)	Has been tested to meet the requirements of MIL-P-43607, "Padlock, key-operated, high-security, shrouded shackle"
SMILS (MK6, MOD 0, 1, and 2)	High-security modular lock designed to secure shipboard hatches and scuttles. Also has land-based applications.	Available from NSWC, Crane, IN
APPROVED REPLACEMENT CYLINDER		
5340-01-449-4349	MEDECO cylinder, high-security w/ R1 keyway supplied with 2 operator keys and one control key	For S&G 833C padlocks. Used by non-DoD federal agencies and Government contractors
5340-01-323-1087	MEDECO cylinder, high-security w/ D4 keyway supplied with 2 operator keys and one control key	For S&G 833C padlocks. Used by military and DoD

APPROVED HASPS			
Nomenclature	**Application**	**NSN**	**Mil-Specification**
MK II, MOD IX, Style 1 (NAPEC 957)	Right-hand style for use on sliding and hinged doors (Figure 5-4)	5340-01-196-2547	MIL-H-29181
MK II, MOD IX, Style 2 (NAPEC 958)	Left-hand style for use on sliding and hinged doors	5340-01-235-6907	MIL-H-29181
1300 Series-Basic	Shipboard, for use with MIL-P-43607 padlocks that have been modified by removing the shackle (Figure 5-5)	5340-01-282-7938	MIL-H-24653
1300 Series-Accessory	Shipboard – watertight hatches	5340-01-282-8275	MIL-H-24653
Anti-Intrusion Box (NAPEC 0963)	Left or right-hand hinged doors. Fits over NAPEC 957/968 hasp. (Figure 5-6)	(Available from NSWC, Crane, IN)	
Universal Security System (NAPEC 1332)	Left- or right-hand sliding doors (Figure 5-7)	(Available from NSWC, Crane, IN)	

*The HI-SHEAR LK 1200 and S&G 831-B High-Security Padlocks no longer meet the requirements of Military Specification MIL-P-43607 and should be replaced as quickly as possible with the S&G 833C, listed in Table 5-2. They can be used until replacement locks are available, but cannot be repaired if a failure occurs. Replacement keys and cylinders are not available for these locks.

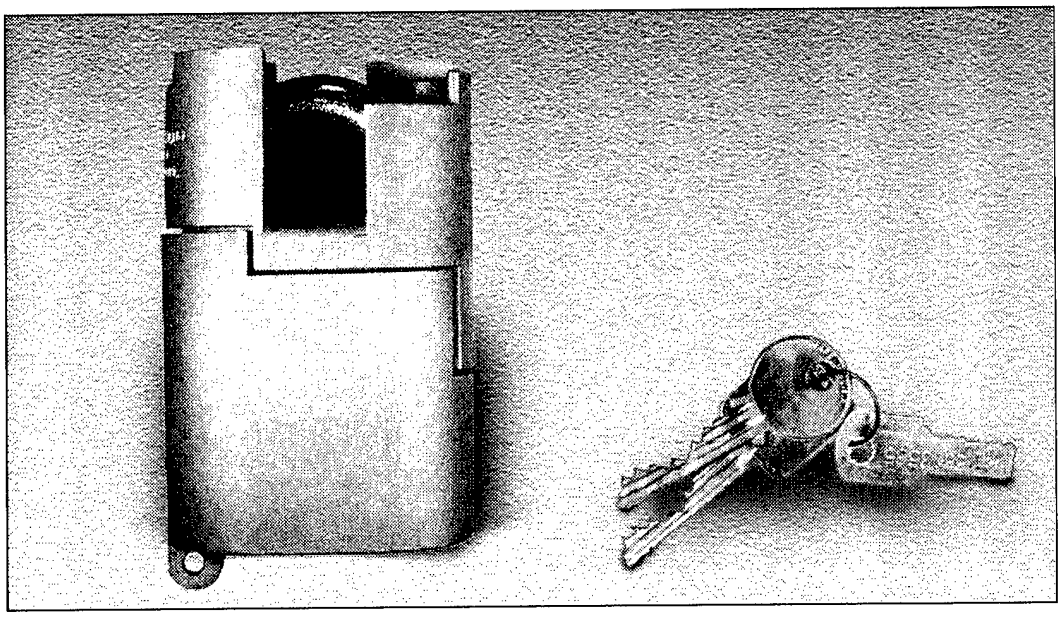


Figure 5-3. High-Security Padlock (S&G 833C)

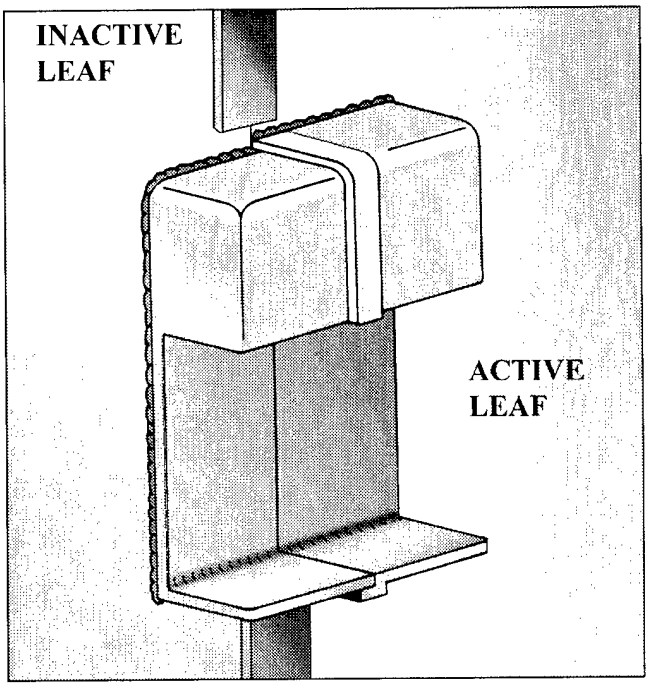


Figure 5-4. High-Security Hasp (NAPEC 957 Right-Hand Opening)

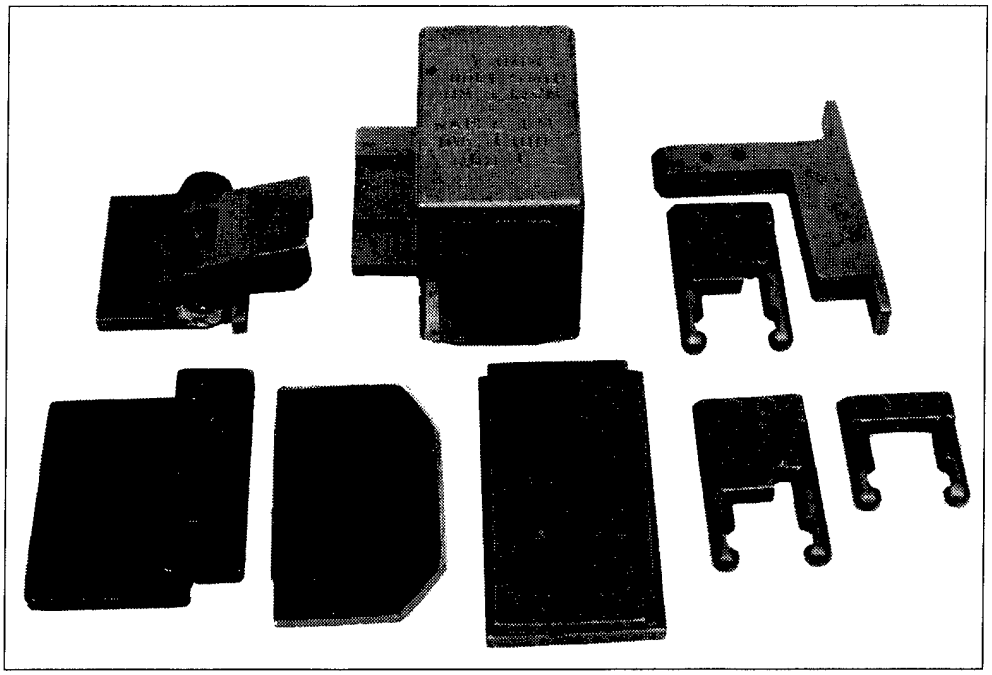


Figure 5-5. Shipboard Hasp (NAPEC Series 1300)

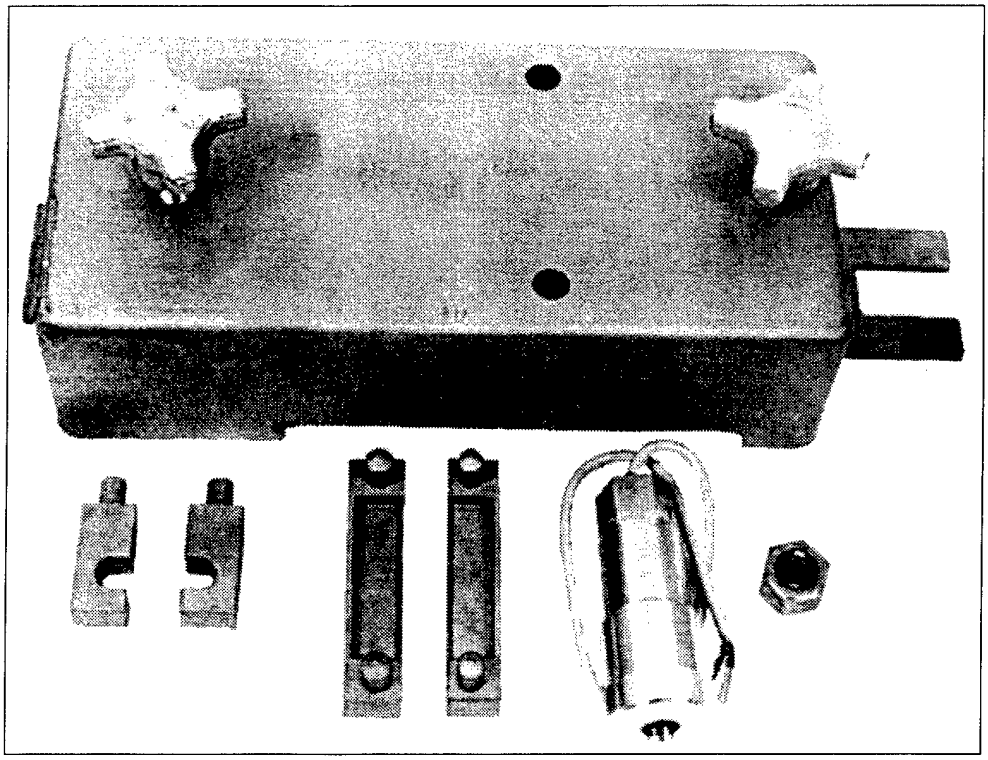


Figure 5-6. Anti-Intrusion Box

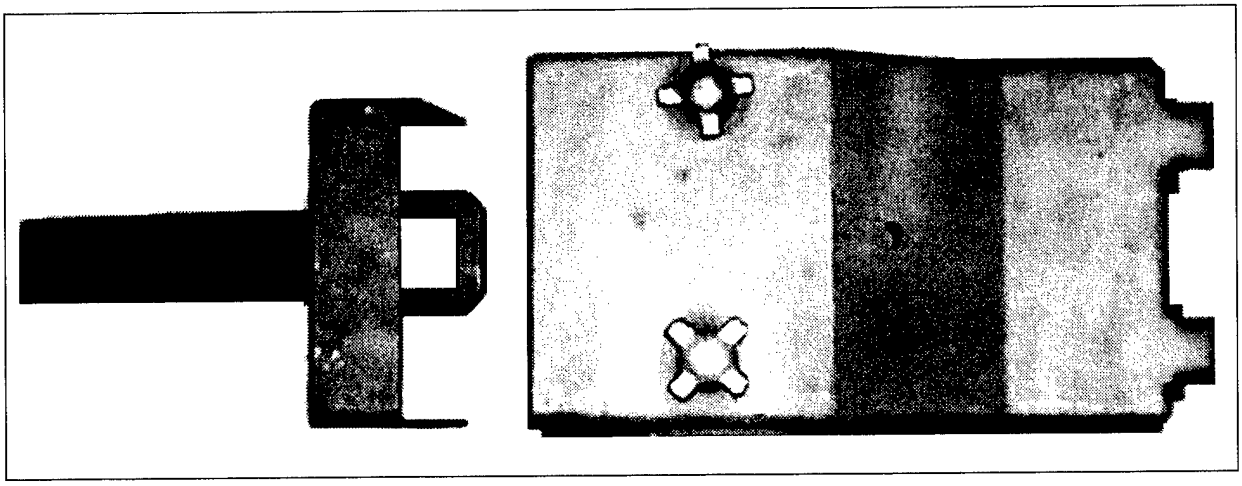


Figure 5-7. Universal Security System (NAPEC 1332)

APPENDIX A

GLOSSARY OF LOCK, KEY AND ACCESS CONTROL TERMS

GLOSSARY OF COMMON LOCK AND KEY CONTROL TERMS

Access Control	A method of controlling the movement of persons into or within a protected area.
ANSI	American National Standards Institute, the coordinator of the U.S. voluntary standards system. The system meets national standards needs by marshaling the competence and cooperation of commerce and industry, standards-developing organizations, and public and consumer interests. ANSI specifications listed in this guide have been adopted by the DoD.
Anti-Passback	An access control software feature that prevents two individuals from using the same access control card to gain access at the same time (i.e., first individual swipes card to gain access then passes the card to a second individual for the same purpose).
ASTM	American Society for Testing and Materials. From the work of 133 technical standards-writing committees, ASTM publishes more than 8,000 standards each year in 68 volumes of the Annual Book of ASTM Standards. The ASTM Committee F12 on Security Systems and Equipment develops and standardizes terminology, test methods, specifications, performance specifications, classifications and practices for security systems, components, and equipment referenced in this guide.
Barrel Key	A key that has a round hollow post and a projecting wing to actuate the tumblers and the bolt of the lock. It is sometimes known as a "pipe key."
Bit Key	A key with one or more wings or bits that project from the round solid post and that operate the tumblers and the bolt of the lock. This key is sometimes referred to as a "wing key" or a "skeleton key." It was once popular in earlier locks used in residential buildings.
Bitting	The cuts in a key that are configured to match the specific tumbler code of a lock or core.
Blade	The part of a key that may contain the cuts and/or milling.
Blank	Any uncut key produced by a manufacturer to fit its own lock keyways or keyways made by other lock manufacturers. It is sometimes referred to as a key blank.
Bow	The portion of a key which serves as a grip or handle.
Building Master Key	A master key that operates all or most master-keyed locks in a specific building.

Change Key — A key that will operate one lock or a group of keyed-alike locks.

Code — The alphanumeric or numerical symbols assigned to a key or lock cylinder that indicate the depth of the cuts and their location on the blade of the key.

Compromise — A security violation resulting in confirmed or suspected exposure of classified information or material to an unauthorized person.

Construction Key — A key supplied with construction-keyed locks. During construction, a builder gains entry using the construction key. On completion of the building, action is taken to render the construction key inoperative (Figure A-1).

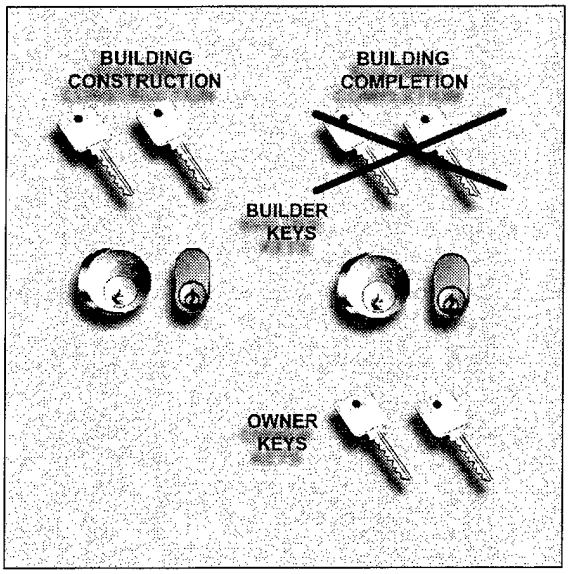


Figure A-1. Construction-Keyed System

Control Key — A key issued by the lock manufacturer for disassembly and maintenance only. Never use this key for normal operation of the lock. In the case of interchangeable core locks, the key is specifically cut for removing and replacing the lock core.

Core — The term is sometimes used as a synonym for plug, but *core* is also used to refer to the figure eight shaped unit that can be removed and replaced in interchangeable core cylinders.

Covert Threat	A threat that uses stealth or deception to gain entry. For access control, examples include picking and bypassing of locks and the use of duplicated or stolen access cards
Cylinder	A complete operating unit that usually consists of the plug or cylinder, shell, tumblers, springs, plug retainer, a cam/tailpiece or other actuating device, and all other necessary operating parts.
Double-Bit Key	A key bitted on two surfaces.
Emergency Master Key	A key sometimes known as a "lock-out key." It is normally used in emergency situations when the door to a hotel or motel room is locked from the inside. When the deadbolt is secured from inside a room, the emergency key is the only key that can unlock the locking device from the outside. It is used in emergency situations only, and if a door is locked with the emergency key, it cannot be unlocked by using any other key.
Enclave	A secured area within another secured area.
Flat Key	A key which is completely flat on both sides, usually used for warded or lever tumbler locks.
Grand Master Key	A key that operates two or more separate groups of locks, each group under a different master key.
Insider Threat	An individual who would take advantage of authorized access to a controlled area to compromise critical information or material to which they may or may not have authorized access.
Hasp	A device that consists of either a hinged plate with a slot in it that fits over a staple or two pieces designed for the shackle of a padlock to pass through to secure the pieces to each other.
High-Security	Locks, hasps, alarms, and security devices, which offer a greater degree of resistance to certain methods of attack. Within the DoD, hardware that has been tested and certified to meet specific requirements stated in Military Specifications.
Key Change Number	The recorded code number that is stamped on the bow of a key that indicates the key change. For example, in the key change number A-2, "A" might mean that the key is assigned to master system A, and the "2" indicates change 2 under the master.
Key Code	A numerical listing that corresponds to the length of individual pins in a key lock. This can be used to cut a key that will operate the lock.
Key Custodian	Individual responsible and designated for safeguarding and accounting for keys and key codes.

Keyed-Alike System — A system that allows a number of locks to be operated by the same key. It is often used in perimeter applications. There is no limit to the number of locks that can be keyed alike (Figure A-2).

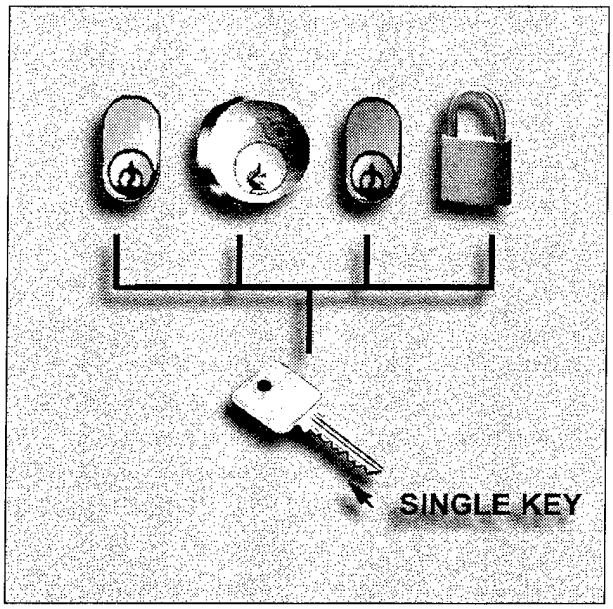


Figure A-2. Keyed-Alike System

Key Indexing — A method of associating every lock/core to a specific key by referring to a coded index.

Keyway — The opening in the plug of a lock cylinder into which the key that operates the lock is inserted.

Maison-Keyed System

A form of a master-keyed system in which each lock has its own individual key that will not open any other office, but all keys will operate the locks to communal entry doors or service areas (Figure A-3).

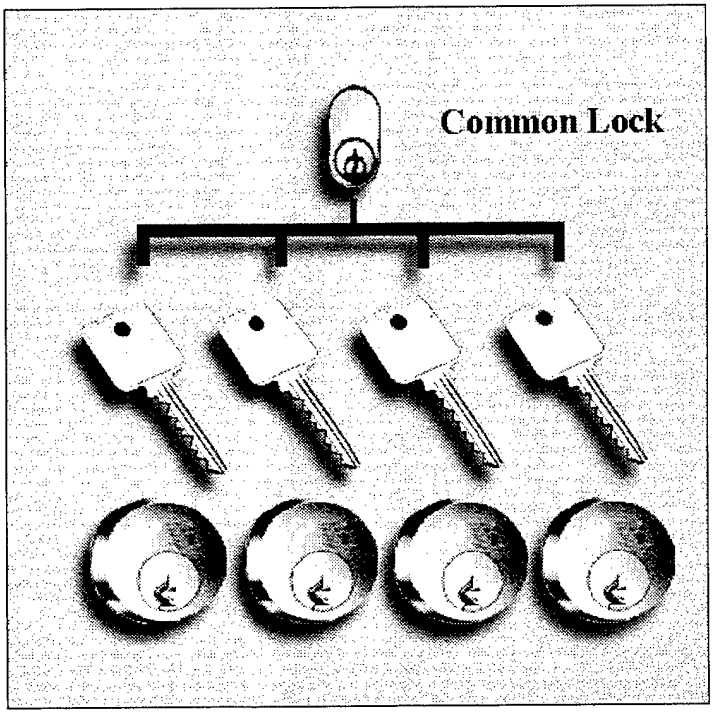


Figure A-3. Maison-Keyed System

Master-Keyed System — A method of keying locks that allows a single key to operate multiple locks. Several levels of master keying are possible: a single master key is one that will operate all locks of a group with individual change keys; a grand master key will operate all locks of the master-keyed system. (Figure A-4).

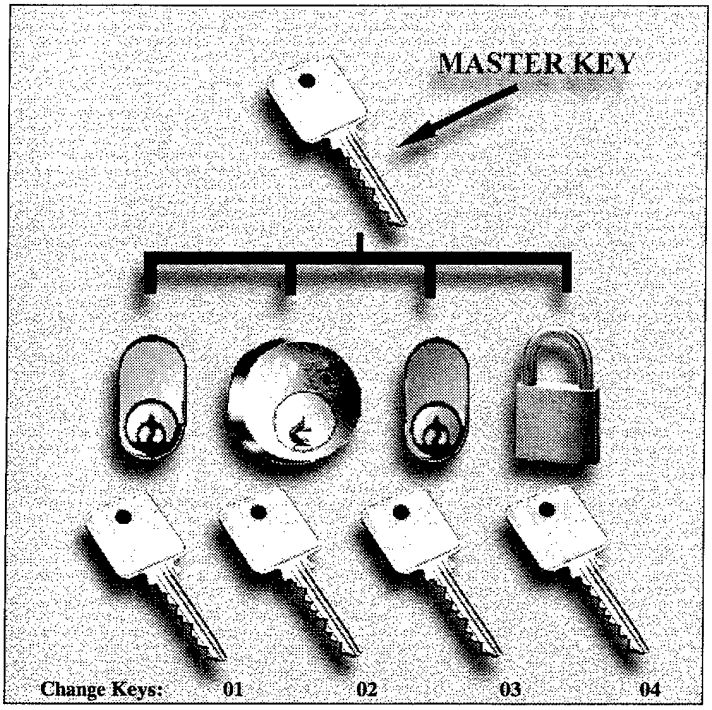


Figure A-4. Master-Keyed System

Padlock — A detachable and portable lock with a shackle that locks into its case. Components performing the same purpose of a shackle but differing in design are sometimes used instead of a shackle.

Paracentric — Of or pertaining to a keyway with one or more wards on each side projecting beyond the vertical center line of the keyway to hinder picking. A term used to distinguish a milled cylinder key from others, such as bit keys and flat keys. The word is defined as "deviating from the center." The term describes the irregular shape of keyways used in pin tumbler locks. The deviation from the center adds to the security of the cylinder, because it makes inserting lock picks difficult, and the bearing surface of the key will assure longer life.

Plug — The rotating, keyway-containing portion of a tumbler or disc type lock or lock cylinder.

Post — The round part of a bit key to which the wing or bit is attached.

Preauthorization	The previously established right to enter a controlled or restricted area.
Preventive Maintenance	Scheduled periodic inspection, cleaning, repair, and lubrication of equipment to ensure continued performance in a working environment.
Push Key	A key that performs its function of aligning the tumblers with the shear line by inward rather than rotary motion.
Restricted Keyway	A special keyway configuration that is not freely available and that must be specifically requested from the manufacturer.
Rekey	Changing the core or pins in a cylinder to prevent a previously issued key from opening the lock.
Security Container	A container usually equipped with a mounted combination lock specifically designed for protection of classified material or sensitive items.
Service Life	Amount of time in which the product meets or exceeds the performance criteria for which it was designed.
Shackle	The part of a padlock that passes through an opening in an object or fits around an object and is ultimately locked into the case.
Shank	The part of a bit key between the bow and the stop; or, if there is no shoulder stop, the part between the bow and the near side of the bit.
Shoulder	The flat portion at the end of the bow on most keys.
Stem	The rounded portion at the end of a shank of a bit key to which the wing or bit is attached. The part forming the axis, on which a bit key rotates in the lock, is also referred to as the post.
Surreptitious Entry	A method of entry which would not be detectable during normal use or during inspection by a qualified person.
Tailgating	A specific method of gaining entry. Access is achieved by walking or driving immediately behind an authorized individual or automobile with a valid access card to gain entry before the entry point has been allowed to close. Tailgating is also referred to as piggybacking.
Throughput Rate	The maximum number of people that can enter an area in a given time period.
Two-Person Rule	A policy that requires two people to be present when an area or asset is accessed.
Underwriters Laboratories, Inc.	A national testing laboratory that tests, lists, and labels various categories of equipment for safety and reliability. They also publish standards for a wide range of products, including security products.

APPENDIX B

REFERENCES

LIST OF REFERENCES FOR LOCK AND KEY CONTROL

1. DoD 5100.76-M, Department of Defense, "Physical Security of Conventional Arms, Ammunition and Explosives."

2. OPNAVINST 5530.13, Department of the Navy, "Physical Security Instruction for Conventional Arms, Ammunition and Explosives."

3. OPNAVINST 5530.14, Department of the Navy, "Physical Security and Loss Prevention Manual."

4. OPNAVINST C8126.1A, Department of the Navy, "Nuclear Weapon Security Manual for Command, Control, Communication and Intelligence," 20 December 1994.

5. AR 190-11, Department of the Army, "Physical Security of Arms, Ammunition and Explosives."

6. AR 190-51, Department of the Army, "Physical Security of Unclassified Army Property (Sensitive and Nonsensitive)."

7. AFI 31-209, Department of the Air Force, "Resource Protection Program."

8. AFMAN 31-224, Department of the Air Force, "Resource Protection/Security, Facilities and Equipment."

9. Naval Facilities Engineering Service Center, "Antipilferage Seal User's Guide," by the Department of Defense Lock Program, Port Hueneme, CA 93043, October 1997.

10. AR 190-59, Department of the Army, "Chemical Agent Security Program," 27 June 1994.

11. DoD 5210.41M, Department of Defense, "Nuclear Weapons Security Manual (NOTAL)," 9 March 1983.

12. "Master Keying by the Numbers" by Billy B. Edwards Jr., CML, Dallas, TX, RSG Publishing Corp., 1990

APPENDIX C

SAMPLE LOCK AND KEY CONTROL PLANS

SAMPLE LOCK AND KEY CONTROL PLAN FOR AA&E

5530
(date)

(Facility) Instruction _____

From: Commander

Subj: LOCK AND KEY CONTROL PLAN FOR AA&E

Ref: (a) DoD 5100.76M
(b) OPNAVINST 5530.13

Encl: (1) Initial Key & Lock Inventory
(2) Daily Key Log
(3) Monthly Key and Lock Inventory
(4) (Additional forms desired by facility commander)

1. Purpose. To establish a lock and key control program for (facility), in accordance with references (a) and (b).

2. Scope. Included in this plan are all keys, locks, padlocks, and locking devices used to protect or secure restricted areas for AA&E storage facilities.

3. Definitions. (As applicable to using command. See guide definition list in Appendix A.)

4. Procedures.

   a. Key Control for AA&E. A lock and key custodian will be appointed in writing and is responsible for maintaining a key control log to ensure continuous administrative accountability for keys. Accountability records shall contain the signature of the individual receiving the key, date and hour of issuance, serial number or other identifying information for the key, signature of the individual issuing the key, date and hour the key was returned, and signature of the individual receiving the returned key. Completed key control logs shall be retained in the unit files for a minimum of 90 days and then disposed of according to established procedures for destruction of classified information.

      (1) Keys to AA&E storage buildings, rooms, racks, containers, and intrusion detection systems shall be maintained separately from other keys and be accessible only to those personnel whose official duties require access to them. A current roster of personnel with authorized access shall be kept

within the section, branch, division, or department. The roster shall be protected from unauthorized access.

(2) When arms and ammunition are stored in the same areas, keys to those storage areas may be stored together, but separately from other keys. The number of keys shall be held to the minimum essential. Keys may not be left unattended or unsecured at any time. The use of a master key system is prohibited for AA&E storage.

(3) When individuals, such as duty officers, are charged with the responsibility of safeguarding or otherwise having keys immediately available, they shall sign for a sealed container of keys. When the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. If the seal is found broken, an inventory of the container's contents will be conducted and the Security Officer will be notified immediately.

(4) Keys to AA&E storage facilities will always remain at the facility and shall be returned immediately after the storage facility is secured.

b. Key Storage. For Category III and IV AA&E, keys will be stored in containers made of at least 20-gauge steel, or material of equivalent strength, and equipped with a UL 768 listed built-in, Group 1, changeable combination lock or a GSA-approved combination padlock (S&G Model 8077). Keys for Category I and II AA&E will be stored in a Class 5 GSA-approved security container.

c. Lost, Misplaced, or Stolen Keys. In the event of lost, misplaced, or stolen keys, the affected locks, cylinders, or cores to locks shall be replaced immediately. Replacement or reserve locks, cores, and keys shall be secured to prevent access by unauthorized individuals.

5. Locks and Seals.

a. Locking Devices. Approved locking devices are listed in Enclosure (____).

b. Rotation and Maintenance. High-security padlocks and lock cores/cylinders will be rotated at least annually. This guards against the use of illegally duplicated keys and affords the opportunity for regular maintenance to avoid lockouts or security violations due to malfunction caused by dirt, corrosion, and wear. Locks will be replaced immediately if keys are lost, misplaced, stolen, or otherwise compromised. The testing, inspection, and maintenance of all high-security padlocks and keys will be conducted annually by locksmith personnel.

(1) Maintenance, testing, and lubrication will be coordinated with normal production/work schedules to minimize disruption.

(2) All maintenance, testing, and lubrication will be performed using only approved procedures.

c. Padlock Security. When an AA&E storage structure is open, the padlock will be locked into the hasp or other nearby securing point to preclude the switching of the padlock.

d. Procurement of High-Security Locks. All locks used for high-security applications will meet military specification MIL-P-43607. All high-security lock procurement must be approved prior to issue.

6. Inventories.

a. AA&E Keys and Locks. Inventories of keys and locks shall be conducted semi-annually using the approved form found in enclosure (1). Inventory records shall be retained in unit files for a minimum of 1 year and then disposed of in accordance with established procedures set forth in reference (e).

(signature)

Distribution:

SAMPLE LOCK AND KEY CONTROL PLAN

(Facility) Instruction _____

From: Commander

Subj: LOCK AND KEY CONTROL PLAN

Ref: (a) OPNAVINST 5530.14B
(b) OPNAVINST 5510.1H

Encl: (1) Initial Key & Lock Inventory
(2) Daily Key Log
(3) Monthly Key and Lock Inventory
(4) (Additional forms desired by facility commander)

1. Purpose. To establish a lock and key program for (name of command) in accordance with references (a) and (b).

2. Scope. Included in this plan are all keys, locks, padlocks, and locking devices used to protect or secure restricted areas, security facilities, classified material, and sensitive materials and supplies. Approved locking devices for the protection of classified materials are specified in reference (b). Not included in this program are keys, locks, and padlocks for convenience, privacy, administrative, or personal use.

3. Procedures.

   a. Key Control. The Key Control Officer/Security Officer shall be designated in writing by the Commander. The Key Control Officer/Security Officer shall hold a security clearance equal to the highest level of classified material held by the command. The Key Control Officer will institute a program that indicates all keys on hand, keys issued, to whom, date keys were issued and returned, as well as signatures of persons drawing or returning security keys. Access to the Key Control Locker must be controlled, and the locker must be secured when not in use. Duplicate keys will be provided protection equivalent to the asset or area that the original keys are used to secure. Continuous accountability of keys is required at all times. The Key Custodian may have an alternate designated, if operationally necessary for mission accomplishment. The name, code, and telephone number of the alternate will be provided to the Key Control Officer and the Physical Security Officer. All forms [enclosures (1) through (4)] are to be used for key accountability and control. Completed key control logs will be maintained in command files for a minimum of 90 days and then disposed of in accordance with established procedures.

b. Criteria for Issuing Keys. Keys for security locks and padlocks may only be issued to those persons with a need for them, as approved by the Deputy Commander or Chief Staff Officer. Keys will not be issued to a member on the basis of his/her status or rank, nor for personal convenience. Certain categories of security assets have specific rules concerning the issue and control of keys affording access to them. The Key Control Officer is responsible for enforcing those rules.

c. Lost, Misplaced, or Stolen Keys. In the event of lost, misplaced, or stolen keys, cylinders, or padlocks, the Key Control Officer and Physical Security Officer will be notified immediately, and the affected cylinders, locks, or cores to locks shall be replaced immediately. Replacement or reserve locks, cores, and keys shall be secured to preclude access by unauthorized individuals.

d. Key Storage. When not attended or in use, keys shall be secured in containers made of at least 20-gauge steel, or a material of equivalent strength, and secured with a locking device or a GSA-approved, three-position, changeable combination padlock, S&G Model 8077.

4. Locks.

a. Locking Devices. Approved locking devices are listed in reference (b).

b. Maintenance. Regularly scheduled maintenance, testing, and lubrication will be performed on all locks. Regular maintenance of all locks is necessary to prevent malfunctions caused by dirt, corrosion, and wear. Testing, inspection, and maintenance on all locks are to be performed annually. All maintenance, testing, and lubrication will be performed using approved procedures.

c. Padlock Security. When the door, gate, or other equipment that a padlock is used to secure is open or operable, the padlock shall be locked onto the hasp, fence, fabric, or other nearby security point to preclude the switching of the padlock.

5. Inventories. The Key Control Officer shall conduct an annual inventory of all keys issued. He/she will also inventory, on a monthly basis, any keys that may have been sub-custodied. All keys shall be inventoried upon change of Physical Security Officer, Key Control Officer or Key Sub-Custodian.

(signature)

Distribution:

APPENDIX D

MECHANICAL AND ELECTRONIC ACCESS CONTROL

INTRODUCTION

This appendix presents information on the component parts of an effective access control system. For access control to work effectively, the access control system must be selected, designed, and integrated to meet the security objectives of the command. In addition, an effective mechanical or electronic access control program must be in place so that integrity is not compromised. Chapter 3 deals with how to establish a lock and key and/or electronic access card control program. The following description of measures can be applied to the design of an effective access control system. The design and integration of access control systems is a complex issue that is beyond the scope of this user's guide.

DEFENSIVE MEASURES

Building layout can be used effectively to defend against covert and insider threats. Because many different situations have been anticipated in developing guidelines, apparent contradictions may occur. Apply the guidance regarding layout where appropriate to the specific situation.

Building Layout to Address Access Control Threats

To limit the number of visitors who must be supervised or escorted, locate facilities with large visitor populations separate from protected assets. Consider using on-site personnel to provide monitoring capability or locate protected assets in common areas where the asset or access to the asset is visible to more than one person. This decreases the probability that unauthorized personnel can gain undetected access to an asset. To reduce the number of access locations that must be monitored, minimize the number of entrances into controlled areas. Building layout considerations also include allocating adequate space for key/access control centers.

Because insiders generally work around the assets, simply establishing controlled areas is not always sufficient. If all employees within a controlled area do not require access to all assets, compartmentalize the assets within the controlled area. For example, if sensitive activities occur in half of a building, that area should have controlled access. When only a few people in the controlled area require access to a particular asset, place that asset in a room within the controlled area and limit access to only those with an established need. Compartmentalization, when used in conjunction with a two-person rule (no single individual can have access to an asset without the knowledge or presence of a second person) provides additional security protection for critical information and assets.

Note: The assessment of alarms from an intrusion detection system (the sensor contact installed on the access-controlled entry point to detect the opening of the door without authorization) may be done by guards or with closed-circuit television (CCTV). A typical, integrated access control system is shown in Figure D-1.

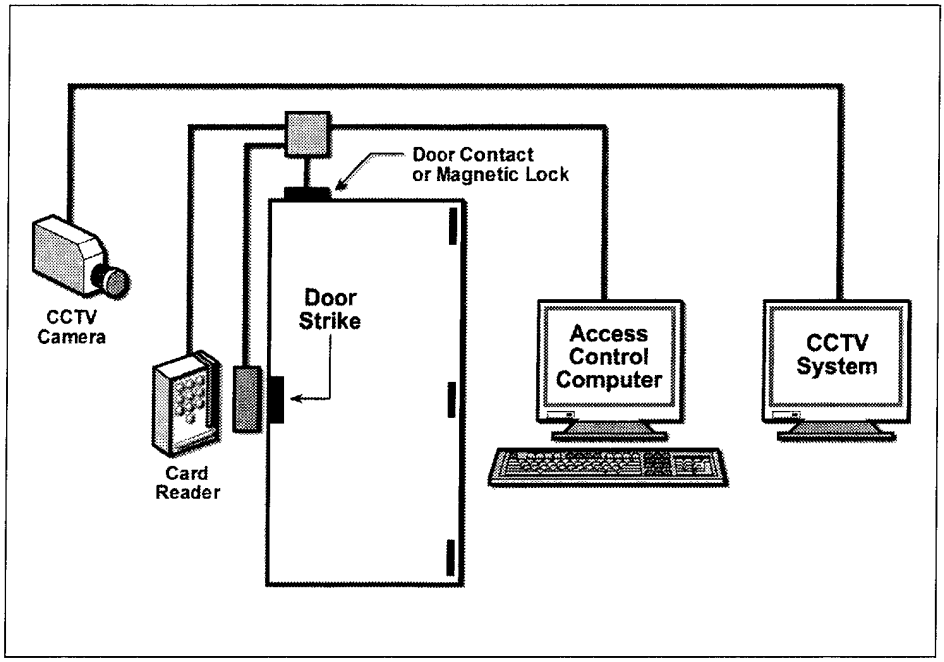


Figure D-1. Typical Simple Access Control System

ACCESS CONTROL SYSTEMS

Access control systems restrict access to an area to those who have received authorization. Techniques used to verify authorization include visual verification of credentials by security personnel; electronic verification of credentials from information known or held by an authorized individual; and the use of electronic biometric identification devices. Throughput rate is an important factor in the design of an access control system to minimize inconvenience to the user. Large throughput rates can be handled with multiple access control units. Access control devices and procedures are described below.

Personnel-Based Systems

Receptionists or security personnel can be effective access control elements, especially for activities with a small staff. For personnel-based systems, locate security posts at the controlled area entrance. Install electric strikes or magnetic locks on entry points that security personnel can activate after verifying identification.

Badging Systems. Badges are entry credentials that must include a photograph of the authorized individual who is issued the badge. The individual keeps the badge and wears it at all times within the facility. Security personnel check identity by comparing the photograph on the badge to the wearer's face. When a controlled area is compartmentalized, the badge should identify specific areas of access. This is usually done through the use of code numbers or colored stripes. Security identification badges have low to medium effectiveness as access control devices in large facilities, because badges are easily counterfeited and procedures used to challenge access (of individuals not wearing badges or those wearing counterfeit badges) are often ineffective. When combined with an electronic access control system however, badges become an effective method for controlling access into a restricted area, because counterfeiting is minimized and bypassing an access control device is difficult without extensive knowledge of electronic systems and use of sophisticated card-duplicating equipment.

Visitor badges represent a significant vulnerability for badge-based access control systems. Visitor badges should be strictly controlled and the use of commercially available, self-expiring, and time-limited visitor badges is highly recommended. Before visitor badges are issued, authorization must be checked and identification verified by picture identification, such as a valid driver's license.

Badge Exchange. To provide more effective control, badge exchange can be used. In this method of access control, an individual receives a primary security identification badge. A second badge different from the first or with different access coding is kept inside the controlled area at all times. When access is required, security personnel exchange the second badge for the individual's primary badge. The individual wears the second badge while in the controlled area. A similar badge exchange takes place as the individual enters each compartmentalized area within the restricted area. When the individual leaves, the exchange process is reversed. This procedure makes counterfeiting difficult, because the intruder would have to gain access to the exchange badges, as well as the primary badge.

Equipment-Based Systems

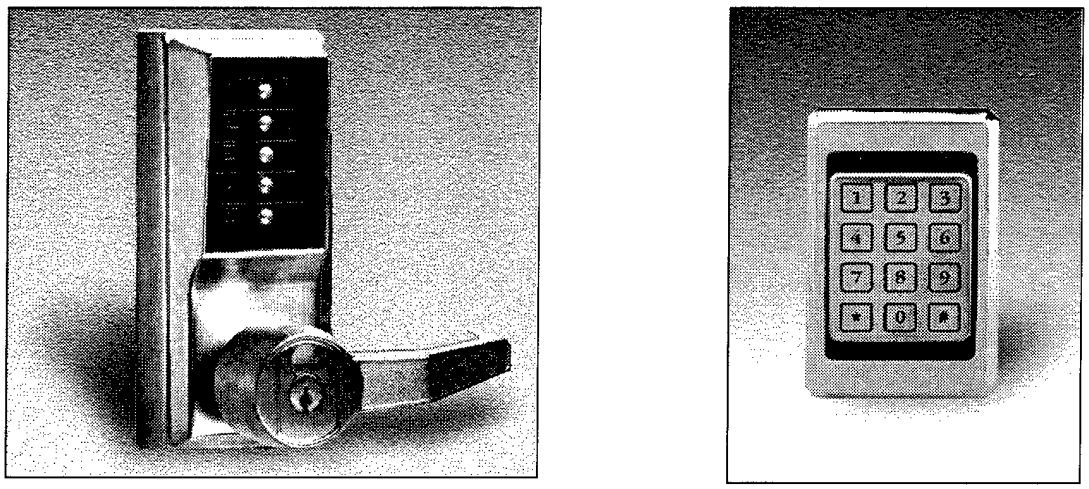
Various types of mechanical and electronic equipment can be installed to allow access to controlled areas not requiring the presence of security personnel. Use of keys and electronic access control cards, and pushbutton mechanical/electrical combination locks are sufficient for low-level access control. Higher levels of protection require secondary credentials, such as a PIN or biometric certification, in conjunction with a card reader and keys/key cards. In addition, strict procedures or equipment must be implemented to prevent tailgating (gaining access by closely following a person with proper credentials). When an authorized individual enters the facility, then passes the card to an unauthorized individual for access using the same card, this is called "passback." This can be controlled through the use of software designed to detect passback conditions. The various types of equipment are described below and are presented in the order of increasing effectiveness.

Mechanical Locks. There are two major categories of mechanical locks, as described by the following:

- Keyed Locks. Keys are the most commonly used and the least expensive way to open locked doors. Key control and key accountability are critical issues if keys are used. See Chapter 3 for guidance on how to establish a lock and key control program.

- Pushbutton Locks. Mechanical pushbutton locks include a keypad onto which an access code is entered, activating the lock to open the door (Figure D-2). These locks are relatively inexpensive but have a high cycle rate and should not be used on entry points requiring a high throughput rate. One advantage of using access codes is that, unlike keys, they cannot be lost and subsequently found by unauthorized individuals, unless the access code has been written down. Their primary disadvantage is the ease with which the access code can be passed to unauthorized people or covertly compromised by simple observation of the entry process.

Electromechanical Locks. Electromechanical locks include an electronic keypad (Figure D-2) that is connected to an electric strike, lock, or magnetic lock. When the access code is correctly entered, the strike or lock is released to open the door.



Mechanical Electronic

Figure D-2. Typical Mechanical Pushbutton Lock and Electronic Keypad

Automated Access Control Systems. Automated access control systems grant or deny access, based upon prior approval of authorization criteria encoded into an electronic access control card. This approval authorization sequence is information that communicates with the equipment, in a format acceptable to the electronics, and provides the criteria for ingress or egress. In general, a multi-door automated access control system is composed of a central controller, an enrollment console, an event video or hard copy display, and entry points controlled by a coded credential and reader (Figure D-1). The primary advantage of these systems is that they are difficult to bypass, compared to conventional lock and key systems. If a badge is lost, it can be voided easily by deleting identification data from the system. The central

processor constantly monitors the condition of remote readers, and access activities are logged on a permanent record.

Stand-alone access control systems (Figure D-3) are battery-powered, and the controller and enrollment components normally consist of a hand-held palmtop or laptop computer. The primary use of single-door systems is at locations where access control is the primary requirement and integration with an alarmed response is not necessary. These stand-alone systems are easy to use, simple to install, and relatively inexpensive, because they do not require the installation of data transfer and power lines.

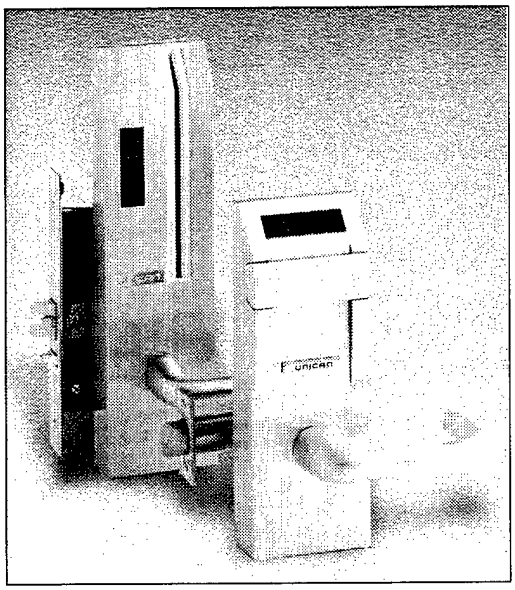


Figure D-3. Single-Door Access Control Systems

ELECTRONIC ACCESS CONTROL SYSTEMS

Access Control Cards

Access control card systems are categorized according to their resistance to copying, decoding, and duplication. Examples of typical access control card systems are shown in Figure D-4. Electronic equipment designers and manufacturers are making major strides in developing innovative devices for access control. Consequently, new security technology is reaching the marketplace on an almost daily basis. Card systems of low, moderate, and high resistance to copying, decoding, and duplication that are currently available are described and listed by category as follows:

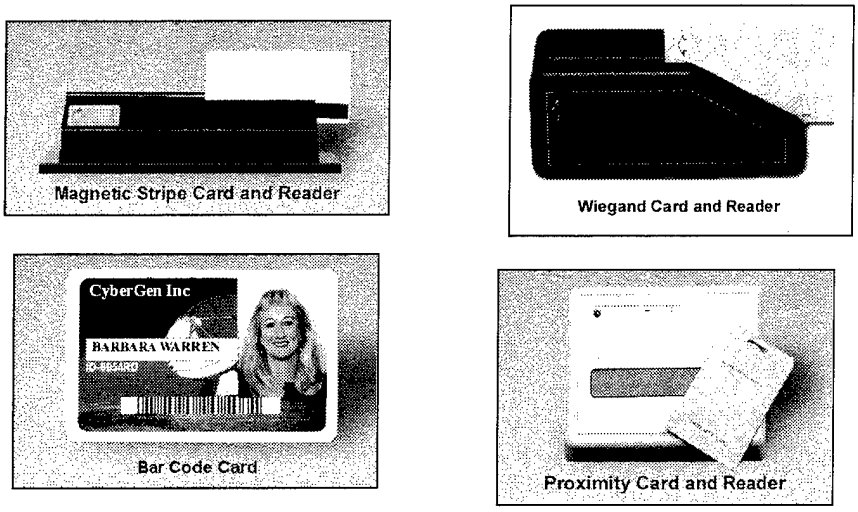


Figure D-4. Examples of Typical Access Control Card Systems

Low Resistance

- Hollerith Card. Punched holes, similar to those on a computer keypunch card, are the means of storing information on the Hollerith card. The amount of information that can be stored is quite limited. The storage space available is even less when printing or a photograph is required on the card.

- Magnetic Stripe Card (Figure D-4). This technology is characterized by a strip of magnetic material capable of containing encoded information. The stripe data is encoded in what is called an Aiken Code. The standards for this encoding relate to the relative position of information on the stripe. Magnetic stripe cards are categorized as high-energy or low-energy, depending upon the encoding energies used with this media. The high-energy types are less susceptible to accidental erasure from contact with magnetic fields.

- Electric Circuit Card. This card is essentially a plug-in printed circuit that can present a limited number of unique codes. The unique codes are values of continuity of electrical pathways on the card. The card is decoded and simulated easily with inexpensive, unsophisticated tools. This card is encoded in the factory, but may be assembled by users.

- Bar Code Card (Figure D-4). Bar codes are seen as a set of parallel thick and thin black lines. These lines form a light/dark pattern that is interpreted by an optical reader or scanner as a code number. Bar codes printed directly on access control cards provide the least expensive, easiest-to-use system in electronic access control identification.

Moderate Resistance

- Metallic Strip Card. This access control card consists of a matrix of metal (usually copper) strips that are laminated to a badge core. The presence or absence of strips can encode a moderate amount of information. The card is factory-encoded, but it may be assembled locally to add custom artwork and photographic images.

- Magnetic Spot Card. This access control card is plastic laminated and incorporates a sheet of ferromagnetic material with spots strongly and permanently magnetized on the core material. Caution should be exercised when placing this card with bankcards or magnetic tape/stripe media due to the other cards' susceptibility to erasure. The card is manufacturer encoded, but it may be assembled on-site for photograph or custom printing additions.

- Optical Card. Access control cards that have rows of spots or lines that change under specific illumination are optically encoded. The general optically encoded card contains spots or lines that absorb, transmit, or reflect infrared or another specific light spectrum. This constitutes the unique code that is facility- and card-specific. The encoding is manufacturer-processed, because custom printing must account for specific ink colors that are critical to the read technique.

High Resistance

- Active Electronic Card. This miniature transmitter contains an individual code that is sent when energized by the reader. The media is characterized by a very limited amount of information storage.

- Capacitance Card. The capacitance access control card contains an array of capacitor plates that are connected (or not) in a specific pattern. This pattern is the limited information code.

- Proximity Card (Figure D-4). Proximity access control cards are essentially tuned (passive) antennas, laminated within the core of a card. A weak radio signal is spectrum-generated by the card reader and is attenuated and reflected to the reader as specific information. The information on the card can be decoded.

- Wiegand-Effect Card (Figure D-4). The Wiegand access control card contains a series of small parallel wires laminated within the card. These wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. The wires' placement above and below a critical centerline determines the specific information in binary code. This technology is factory-encoded and, therefore, impossible to erase and difficult to alter or duplicate.

- Contact Memory Buttons (Figure D-5). A contact memory button is a computer chip armored in a stainless steel can that usually resembles a button. These chips have up to 64K of computer memory that can store text or digitized photos. This information can be downloaded or updated as often as needed with a simple, momentary contact with the reader device. They are ideal for applications where information needs to travel with a person or object. They can be used to provide access, carry essential information during a process, or as an electronic asset tag. Their uses are similar to that of Smart Cards, but the memory buttons are packaged for durability, so they can be used in rugged or harsh environments.

- Mixed Technology. This type of access control card combines a variety of technologies, including proximity, magnetic stripe, microprocessor (smart card), Wiegand, etc. Mixed technology cards can be used on a variety of readers, which eliminates the need for carrying a number of cards at a facility with different reader systems. They also make it unnecessary to retrofit a facility to take advantage of new technologies. Smart cards make biometric verification faster and more practical by storing the information on the card, rather than in a computer.

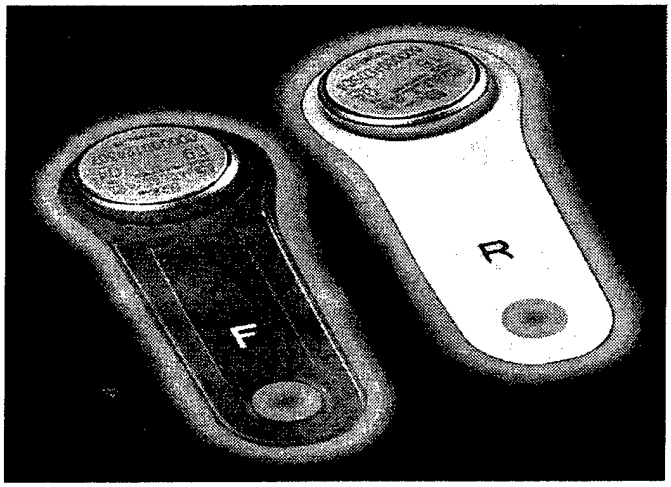


Figure D-5. Examples of Contact Memory Buttons

Badge Reader

Information encoded on a badge must first be decoded or read. It is then transmitted to a processor that grants or denies access, based upon a comparison of the encoded information with authorization files.

A reader is composed of a card sensor and an electronic interface (Figure D-6). The card sensor detects the presence of the coded credential and reads the data. The electronic interface converts the data read by the card sensor into proper format and sends it to the controller. The controller also returns a command to energize a relay that allows access.

Two types of readers are commercially available. The first type has both the card sensor and the electronic interface housed in one unit. The second type of reader has a separate card sensor and electronic interface. The card sensor is mounted separate from the electronic interface and is connected by a short length of cable. State-of-the-art readers contain microprocessors or large-scale, integrated circuits that can perform many other sophisticated functions such as data communication, line supervision, fail-safe operation, and PIN verification.

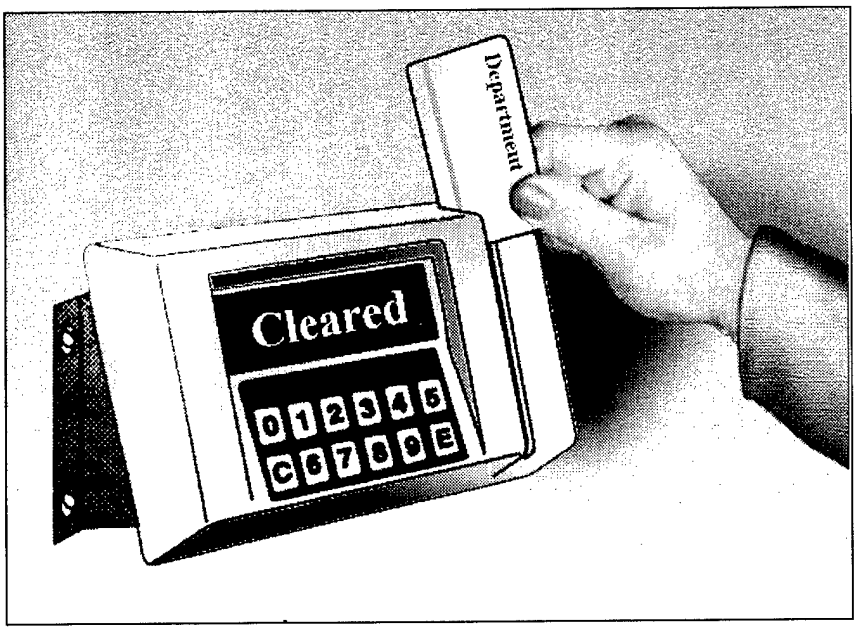


Figure D-6. Card Reader with PIN Entry

Secondary Credentials

All card access badges are susceptible to alteration, decoding, and duplication or loss. The degree to which the technology and associated procedures resist these threats is important to the integrity of the security system. For more critical access verification requirements, additional verification systems, requiring either a code to be entered on a keypad or physical characteristic confirmation, may be advisable as a backup to card-only access authorization. The second verification is to minimize the vulnerability associated with insider collusion and lost or stolen cards. Examples of secondary verifications are PIN, photographic image match-up to files of personnel, hand geometry, fingerprints, handwriting, speech, weight, and other biometric systems (Figure D-7).

Secondary systems, with the exception of biometric systems, are less secure than coded credentials. This is due to the easily read identification media and the wide latitude needed to accommodate variations due to environment, stress, and other data-entry errors that may deny access to authorized users. **A PIN is the most commonly used secondary verification system because of the relative ease with which it obtains an accurate specific data entry and the immunity of this data to environmental influences.**

Figure D-7. Biometric Identification System (Hand Geometry)

The use of a secondary means of access authorization generally should be limited to selected mid-level security applications (see Chapter 1 for definitions), because throughput rates and cost concerns need to be controlled. Systems, now commercially available, display various error rates and this data should be considered in design analysis phases of access control system development. Options available for secondary credential systems include the following:

Personal Identification Number (PIN). For card access systems with PIN options, the readers have keypads where the PINs can be entered. In most cases, the PINs are not stored in the central controller's memory, but are derived from the credential identification (ID) numbers, following some encryption algorithms. In this case, the reader matches the entered PIN with the calculated number to validate the coded credential before it sends the data to the central controller. The preferred method is a system that either assigns a PIN or allows users to select their own PIN that is not related to the badge ID number. Personal identification numbers are vulnerable to covert discovery by unauthorized personnel via visual observation of the keypad entry sequence or poor control of code numbers by users.

Video Comparator Systems. The use of a video comparator system requires a guard to verify an individual's identity, based on visual characteristics. An electronically stored image is used for comparison with a real-time image of the individual requesting entry. Although video comparators are not positive personnel identity verification systems, they have an advantage over

manual photo ID systems in that it is difficult to tamper with the stored image used in the comparator system. Nevertheless, they are categorized as having a low resistance to counterfeiting. In this sense, the video comparator is comparable to the badge exchange system. Enrollment capacity is the maximum number of images that can be stored by the system. The system's access time is the time elapsed from identification number entry until the stored image is displayed for viewing.

Hand Geometry. The measurement of relative finger length is a unique characteristic. Hand geometry is a distinct measurable and individual characteristic. These systems are characterized as having high to medium resistance to tampering.

Handwriting. Signature verification has been used for many years by the banking industry. However, signature comparison methods employed are highly susceptible to forgery. Automated handwriting verification systems have been developed that use handwriting dynamics, such as velocity, acceleration, and pressure as a function of time. Statistical evaluation of this data indicates that an individual's signature is unique and reasonably consistent from one signature to the next. Systems have been developed that use from one to three axes of dynamic measurements. Transducers can be located in either the writing instrument or tablet. Like hand geometry, signature verification has a high to medium counterfeiting resistance level.

Speech. Speech is a useful attribute for identity verification, and it is well suited to automated data processing. Speech measurements that are useful for speaker discrimination include waveform envelope, voice pitch period, relative amplitude spectrum, and vocal tract resonant frequencies (formats). High-end systems have a high resistance to counterfeiting; however, some low-end systems can be fooled with high-quality recordings.

Fingerprint. Fingerprints have been used as a positive personnel identifier for more than 100 years and are still considered one of the most reliable means of distinguishing one individual from another. The art of processing human fingerprints for identification has been greatly enhanced in recent years by the development of automated systems. These systems, which rely on pattern recognition of either a single finger or several and computerized data processing, have an application in access control. All fingerprint identification systems require accurate finger positioning and pattern measurement for reliable identification. Some problems occur with individuals that do not have clearly defined finger ridge patterns or who have had an injury to the identifying finger. Fingerprint systems have a high resistance to counterfeiting.

Palm Print. Palm print recognition systems measure features of the palm or identify the pattern of blood vessels below the surface, or both. Palm print readers are fairly easy to use and do not carry the emotional connotations of fingerprint ID systems. However, they are more cumbersome than fingerprint readers and some practice is required before their use becomes natural to the user.

Eye Scan. Eye-scanning systems measure the retina or iris and are very difficult for the user to circumvent. More advanced systems use a charge-coupled device camera, which is unobtrusive and requires little action on the user's part. Because the scan involves shining a

light into the retina, one potential problem with these devices is that, on a routine basis, they may irritate the user's eye. Employees have shown resistance to eye-scanning systems for this reason.

Electric Door Locks

Locking hardware that is compatible with automated access control systems includes electric strikes, electric bolts, electric locksets, and electromagnetic locks. Each of these devices is available with one of two features, termed "fail-safe" or "fail-secure," and configured in either alternating or direct current in a range of 6 to 240 volts. The design of an automated access control system must consider variables that are related to entry point use and the application of local and national fire, life safety, and electrical codes. Examples of electric door locks include the following.

Fail-Safe/Fail-Secure. One of two operations can take place with electric door locks during a power failure. These two operations are termed fail-safe and fail-secure. If the power fails, the lock becomes either safe for access/egress or secure for locked. These operations are usually applied based on fire code, electrical code, or activity regulations. These codes and regulations assume that, in the event of an emergency (fire or other catastrophe), the individual seeking to exit may not be capable of rapid thought and logical reasoning and requires a simple, usually entirely mechanical, means of exit. The spirit of this requirement is to assure that speedy exit is accomplished without having to read directions or depend upon electrical or electromechanical devices that may fail due to the emergency condition. From a security viewpoint, this option must be clearly addressed because it can create vulnerability if procedures are not in place to prevent reentry during alarm conditions.

Electric Strikes. The electric strike (Figure D-8) is the most commonly used electric lock. It comes in a variety of sizes and can replace existing mechanical locks without a great deal of difficulty. The strike, which is the electrically controlled portion of the lock mechanism, is mounted in a doorframe (jamb) and does not require wiring through the door itself. The electronic strike contains a bolt pocket, which is the indent that holds the protruding latch bolt or dead bolt secure in the frame. To open, the strike rotates away from the pocket, providing a path for the bolt to escape. This rotating side is called a pivoting lip or keeper. This device provides a depression or channel that fits the bolt or latch of the lock. The channel catches or releases the bolt, depending upon the lock status. Issues that must be considered when selecting an electric strike include composition of the doorframe, size and shape of the latch bolt, holding force and potential for abuse of the door lock. Heavy-duty strikes are recommendations for access control systems where potential abuse or high traffic volume is an issue. Options for electric strikes include:

1. A latch bolt monitor indicating if the bolt is extended into the strike.

2. A lock cam monitor indicating if the strike is in a locked position.

3. Sensors indicating whether the door is shut.

4. An interlock feature to permit only one door in a series to be unlocked at a time, as in mantrap or energy-conservation foyer applications.

Electric Bolt. The electric bolt (Figure D-9) is fitted on or in the jamb or the door and when activated, protrudes (or in some models, swings) into a strike plate on the adjoining surface. The dead bolt will not give way with spring action and once it is locked in place, it can not be retracted until the electric signal is given to unlock. This device is used generally for interior door applications, because the electric bolt may not meet certain safety code regulations for egress doors.

Electric Locksets. An electric lockset (Figure D-10) provides positive locking by pushing a solenoid-operated bolt or rotating bar into a hole in the door edge. Another option is the electric key-in-knob (or key-in-lever) lock, which electrically releases the knob, allowing retraction of the bolt. Critical alignment is required between the bolt and the locking strike opening.

Electromagnetic Lock. The electromagnetic lock (Figure D-11) consists of an electrically powered magnet and a steel plate. The magnet is mounted to the doorframe in alignment with the steel plate to provide a strong or hardened area in which to apply magnetic force. Most of these devices are inherently fail-safe (opens during power failure), because power is interrupted to unlock, while some are fail-secure (remains locked during power failure) because they maintain power with backup battery supply. Minor variations in door alignment and problems associated with door settling and warping can be addressed by use of this device. Pairs of doors can be secured by a single device, if both swing in the same direction (outswing or inswing).

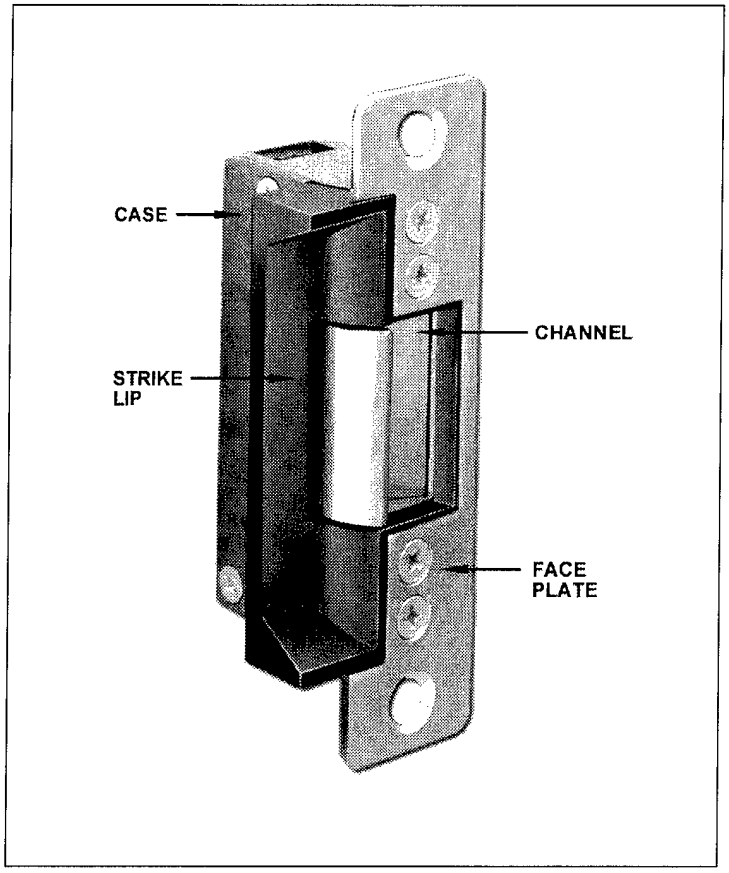


Figure D-8. Electric Strike

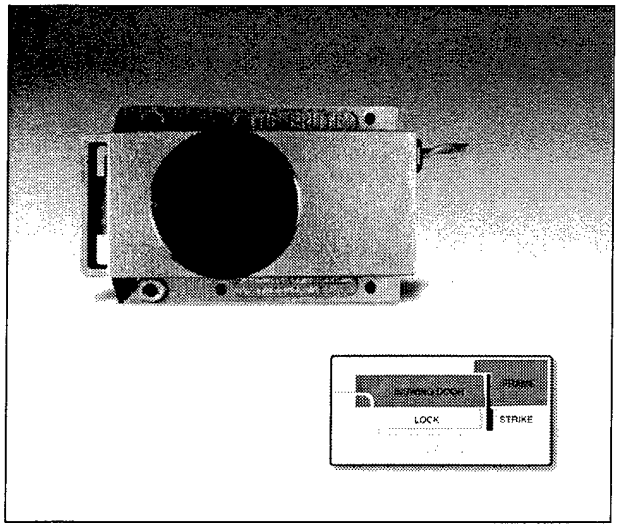


Figure D-9. Electric Bolt

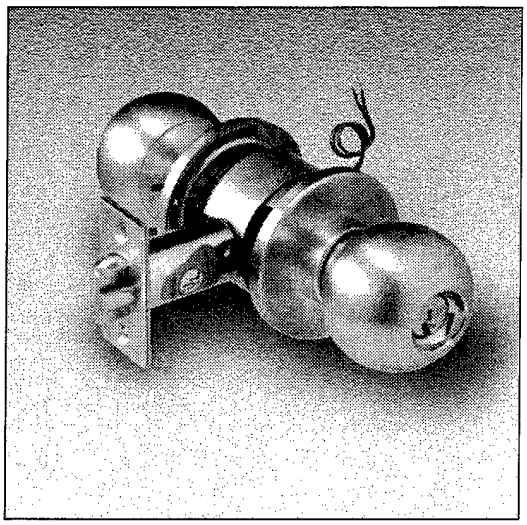


Figure D-10. Electric Key-in-Knob Lock

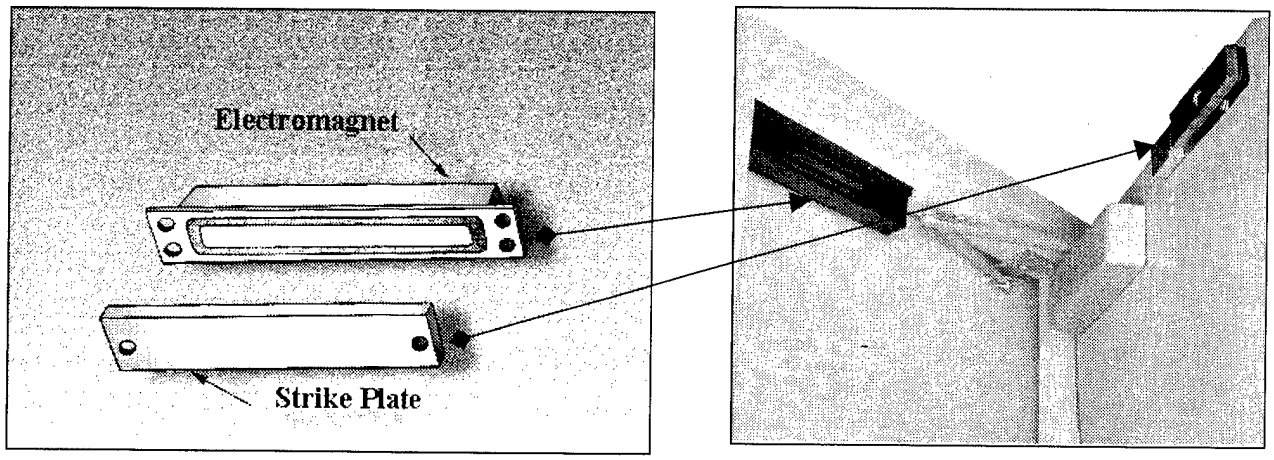


Figure D-11. Electromagnetic Lock

Central Control Unit

The central control unit refers to the main computer that processes and controls information regarding electronic access control authorization and verification. The central control unit consists of a processor or processors and associated peripheral equipment. A typical central controller consists of a microprocessor, read-only memory (ROM), random-access memory (RAM), and magnetic storage memory (disk or tape). The microprocessor executes the computer program stored in the ROM. The RAM contains the access authorization data associated with the enrolled credential number. During normal operation, the central controller receives the incoming credential ID number from the access/entry reader or remote controller and compares it to the numbers stored in memory.

The central controller may also compare the time and location of the requesting credential against the time zone and the area authorization allotted to it. If all information is correct, the central controller gives a go-ahead command to the reader or remote controller and energizes a relay to unlock the door. The central controller records the credential identity number, the date, the time of day, and the reader or door number through which access took place. Conversely, if any information is incorrect, the system rejects the credential, entry is not permitted, and the system issues an appropriate warning message. The time for one transaction is usually less than three seconds. Depending upon the system design, there are many techniques for transmitting data between the reader and the central controller. The most common technique is to transmit the data digitally. Such data can be transmitted for a distance of one mile or more without degradation. Furthermore, by using a modem or newly developed cellular interface, data can be transmitted for an unlimited distance.

Remote Control Units

The remote control unit is that component of the access control system that translates communications and performs interface tasks between credential readers, electric door locks, and

the central control unit. This intermediate device is usually subject to distance constraints and is often located to accommodate line length from readers and the central control unit. The function of a controller includes interpretation of coded information to the central control unit. The controller may also supply conditioned power to the reader.

Enrollment Console

The enrollment console is the device used to initiate the authorization status of an encoded badge. The enrollment console may contain information on badge authorization and can include badge number, employee number, name, address, telephone number, motor vehicle registration, status, issue date, return date, authorization center, and entry point restrictions by time zones, entry/exit status, and trace. A commentary section may also be included for emergency call lists and other safety-related information. Enrollment equipment and equipment used for transferring the data to the central control unit must be located in a secured area. The enrollment console usually consists of a keyboard, badge reader, and a video display terminal. Changes of high authorization levels must be password- or software-protected to prevent unauthorized use of the system. Passive software protection should be included in all system functions to maintain integrity of the total system. Components of the enrollment console include a central processor and printer.

Central Processor. The central processor makes decisions based on information files entered at the enrollment console. It also communicates with remote controllers and checks the encoded information input against the existing files. The central processor approves access based upon the filed authorizations and creates a historical file of attempted accesses and the manipulations of the existing files. This history may either be recorded electronically in computer storage media or printed on paper for later review.

Other functions performed by the central processor depend upon the system design. At one extreme, only minimal capability is assigned at the entry point and reader. Consequently, data is transmitted to the central control unit, and the central processor makes decisions. At the other extreme, significant capability is assigned at the entry point and reader, and decisions are made locally, which allows faster processing and entry. In all cases, reader status and alarm status signals are sent to the central processor, then transferred to the information display in the guard station.

Printer. The printer is an output device that provides a hard-copy record of activities reported by the central processor. Printers should have sufficient speed and appropriate buffer to avoid information omissions from overload by the much faster system electronics. Security systems do not generally require letter quality printing, so faster printing can be selected for this operation.

Accessories

To extend or enhance the capabilities of a system, accessories may be added to the basic system. Three types of useful accessories are multiplexers, alarm-switch monitors, and computer interface modules.

Multiplexers. A multiplexer accepts input from several readers, patches the signals together, and sends it to the controller. It also receives commands from the controller, then separates the information and routes the commands to the appropriate readers. The multiplexer serves as a concentrating point and is used in conjunction with a remote cluster of readers. Because the multiplexer amplifies the signal, the distance between the controller and the readers can be longer.

Alarm Switch Monitor. An alarm switch monitor checks the status of several switches and reports any change of switch status to the controller. The monitor also enables the card access system to function as an alarm monitoring system that can report events not associated with personnel access. If security operations require the control functions of access and alarm monitoring to be distinct and separate, two systems will have to be developed during design phase.

Interface Module. The computer interface module ties the card access system to an existing computer system. It converts the output of the controller into a proper format and sends it to the host computer. By integrating the card access system into the computer system, the output of the card access system can be stored in a permanent file, or it can be processed and displayed in compatible format.

Automated Access Control System Functions

Computer-based systems permit flexibility in controlling and removing mundane, repetitive tasks from guard responsibility. Computer-based systems can instantly check authorized access data against the access requests and record the event. This automation permits greater efficiency of guard personnel, while potentially reducing the number of fixed posts required and improving security to the facility.

Access Authorization/Verification and Reporting

Approval for personnel to have access to a specific entry point requires advanced approval and system enrollment. Approval or denial of access also requires the system to check for any limitations associated with the encoded credential at the time of each access request. The system operates without prejudice on a repeatable basis. Approval of entry is reduced to a routine task that requires human intervention only in the event of exceptions. The access control system will note and report exceptions and operator-initiated actions. Human failures or errors are controlled, while high throughput for verified access approval is maintained. Use of closed-circuit television (CCTV) and/or voice communication at each access control point allows immediate assessment of exceptions or operator error.

Multiple Area Authorization

Access authorization can be as general as system-wide approval or as specific as an individual entry point. Authorization files should include the appropriate classification of an entry point if it is associated with the perimeter of controlled or restricted areas. The entry point

should be assigned the classification of the restricted area and access allowed only to persons with authorized access to the area and based upon need-to-know principles.

Time Zoning

Access authorization can also be based on time. Access may be approved only if the individual is authorized to access an entry point during a specific time period. Time codes may also be designated to preclude all access during specific time periods (such as at night or weekends) assigned to an entry point. Thus, either individuals or areas may be excluded from access, based upon the definition of time periods. This feature could be used if regular working hours or closed hours have been established at a facility. The criteria include time of day, day of week, and an eight-day calendar (holidays scheduled as the eighth day).

Fail-Safe/Fail-Soft (not to be confused with Fail-Safe/Fail-Secure on page D-13)

If the communication lines between the controller and the central processor are lost, the default parameters within the system are exercised. Two schemes are available to address this problem. The first, fail-safe, prohibits access, even if the criterion of correct facility code is met. The fail-soft scheme, also referred to as degraded mode, normally grants access upon correct facility code entry. A caution must be observed: few systems in the degraded mode record access information for later transmission to the computer when the communication line is restored.

Occupant Listing

An occupant listing is an internal software function that can process entry information and permit access by area, maximum number or load of personnel, or enforcement of the two-person rule. Specific reader configurations and entry and exit readers must be used in conjunction with anti-passback or tailgate (or piggyback) prevention controls. The controls must be used to ensure that accurate data is gathered. The computer can compile valid lists only if all entries and exits are indicated. Requirements such as safety and the two-person rule can be effectively controlled with manipulation of this information. This feature can also play a role in evacuation plans and evacuation assurance.

Anti-Passback

Denial of access or egress approval in the event of two successive "in" or "out" access requests is anti-passback. This denial prohibits the unauthorized use of a single card by two persons until exit readout is accomplished. This avoids the event where one individual obtains access and, while inside, "passes back" the access credential. Tailgating or piggybacking is a fault in automated access control systems in which two persons gain access with one card at the same time. A single authorized card is used and approved, but two persons enter during the entry point access time window. This problem is critical in sensitive facilities, particularly if duress situations are a threat. The problem can be addressed through the use of a rotary gate or turnstile (Figure D-12) connected to and controlled by the access control system or by an interlocking mantrap (Figure D-13) with direct visual security surveillance. Closed-circuit

television assessment, in addition to access control at entry points, the less effective "beam break," and personnel counting devices with appropriate alarm/delay features, should also be used for these applications.

Figure D-12. Turnstile

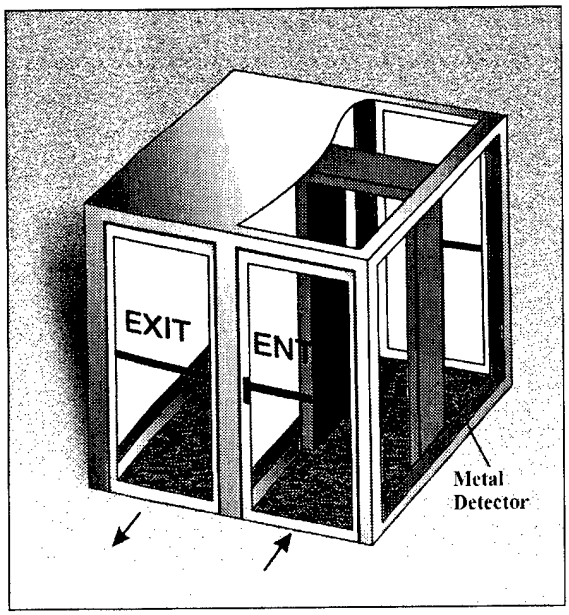


Figure D-13. Mantrap

General Automated Access Control Applications

Several factors directly affect the successful operation of an electronic access control system. System designers must be familiar with limitations and constraints.

The selection of an access control system involves virtually as many factors as there are potential applications. Because selection will generally be commercial, off-the-shelf systems, the two primary considerations are first, the capabilities of the proposed equipment, in terms of local security/use requirements, and second the experience and capabilities of the installation firm to support the equipment during its life cycle. These two factors need to be considered together, because poor installation and service can negate the benefits of the most detailed design process. Maintenance must be examined as part of the life cycle cost of the system.

The standard features of the automated access control system enhance security operations, particularly where the equipment outperforms humans in repetitive functions. This creates a more secure environment, because it allows the human element to perform in the area where greater efficiencies can be achieved. Definition of access, based upon area, access point, time zone, holiday schedule, loading, two-person rule, and the subsequent recording of the information relative to use, can be essential. Automation of electronic alarm processing within one control center provides a single source of information regarding the facility or activity security. Other software enhancements, such as automated guard tours and patrols, redundant life safety system monitoring, security trace, data encryption, and centralized control/reporting, can improve the versatility of the system. The capability of the system to call up electronic commands to address detected events with specific details, telephone numbers, and prioritized sequences further reduces the margin for error by reducing the requirements for human judgment.

Design of the access control system should take into consideration an expansion capability of at least 25 percent with minimum hardware and software additions. The best systems permit additions of equipment to meet expansion, without obsolescence of existing hardware. Modular enhancements in hardware capability permit maximum configuration until the central processor is outgrown and additional or different processors are required. State-of-the-art processing equipment is designed to be implemented in building blocks, with logical breaks, in order to meet individualized usage. Off-the-shelf modules that are system enhancement-oriented often provide the required capabilities cost effectively.

The degree of access level designed into a system is based upon the protected area security requirement, authorized need for access through a particular entry point, and the required resistance to defeating the identity verifier. The throughput rate is the average number of individuals who can pass through an entry point during a specific period of time. Normally, the throughput rate is specified in personnel per minute. The design at the requirements phase should identify all entry points scheduled for control and determine the number of authorized personnel who use each entry/egress control point. The configuration of each control point will be expanded based upon peak throughput requirements, primarily at shift changes. The employment of positive barriers, such as sallyports, turnstiles, or other access limitations, will determine the number of readers required to conveniently process legitimate access. Card credentials alone typically will require 3 to 5 seconds per card when configured properly.

In normal operation, automated access control systems provide a given level of security by restricting unauthorized access. Although this level of security may normally be sufficient,

equipment failure can decrease security to an unacceptable level. Failure of critical equipment may cause total system failure. Efforts must be made to minimize both the impact of system failure and the associated repair time.

APPENDIX E

LOCK AND KEY CONTROL FORMS

Table E-1. Key Inventory Log

KEY INVENTORY LOG		
Page:		Key Control Center Location:
KEY #	**CYLINDER/ CORE #**	**LOCATION SERVICED**

Table E-2. Key Access Log

KEY ACCESS LOG					
Page:		Key Control Center Location:			
NAME (PRINT)	**DEPT. CODE**	**WORK PHONE**	**HOME PHONE**	**EMPLOYEE/MILITARY ID NUMBER**	**SIGNATURE**

Table E-3. Key Control Log

KEY CONTROL LOG

Page:		Key Control Center Location:						
ISSUE		KEYS	KEYS	ISSUED TO:	ISSUED BY:	RETURN		ACCEPTED BY:
DATE	TIME	SERIAL NO.	TOTAL NO.	NAME (PRINT) SIGNATURE	NAME (PRINT) SIGNATURE	DATE	TIME	NAME (PRINT) SIGNATURE

Table E-4. Key Issue Record

KEY ISSUE RECORD

FROM:	TO: Department Key Custodian	DATE:

Requested that

_____

Name Military Grade Employee/Military ID Number

be issued _____ key(s) to the following areas:

(Identify building number, floor and room number, container, cage or section, as applicable)

_____

_____

_____

FROM:	TO: Department Key Custodian	DATE:

STATEMENT OF ACKNOWLEDGEMENT OF RECEIPT OF KEY

I understand that keys issued to me provide access to the space listed above. Additionally, I have read and am familiar with the Key Security and Lock Control Program and understand that the following provisions apply:

a. Duplication of keys, other than those approved by the security manager, is not approved.

b. Keys must remain in my possession at all times and may not be loaned.

c. Upon my transfer or reassignment, the keys must be turned in to the Department Key Custodian.

d. Loss of keys must be reported to the activity police and Key Custodian immediately.

e. It is my responsibility to ensure that all spaces to which I have keys are locked at the end of the day.

f. Keys are property of the U.S. Government.

SIGNATURE_____

Table E-5. Key Manufacturing Request

KEY MANUFACTURING REQUEST

FROM: (Shop or Activity)	TO: Department Key Custodian	DATE:
Number of Sample Keys	Number of keys to be made	Job Order Number
Name of Requester	Title (Head of shop or activity)	

1. These keys (do) (do not) apply to an area under the department key control.

2. This request is submitted:
   ( ) To provide additional keys for a new lock cylinder/core/padlock.
   ( ) To replace lost/missing key(s) for current lock.
   ( ) To provide additional key(s) for current lock.

3. The lock/padlock that this key operates is located in/at:

   Building No. _____ Room No./Name _____

4. The area/room is used for (office, storage, etc.):

_____

_____

_____

5. Identify contents of the area/room that cause it to fall under the key control program:

_____

_____

_____

_____

_____

To be filled out by Key Custodian

FROM: Department Key Custodian	TO: Key Control Officer	DATE:
Approved by: Name (typed)	Signature	

Table E-6. Lock Repair/Service Request

LOCK REPAIR/SERVICE REQUEST		
Requester		**Lock Serial No.**
Date		
Job Order Number	**Code**	**Location**
Point of Contact (if different from requester)		**Phone**
Problem		

WORK DATA (To be filled out by person performing work)	
Item	**Time Used**
Combination	
Repair	
Service	
Modify	
Remarks	

Date Completed	**Completed By**

APPENDIX F

MANUFACTURERS LISTING

NOTE: This is only a partial list. Any reference to a manufacturer is included only to illustrate a piece of equipment. It is not intended to be a recommendation or an endorsement of any product or company.

ALPHABETICAL LISTING OF MANUFACTURERS

MANUFACTURER/ADDRESS/PHONE	PRODUCTS
Abloy Security, Inc., 6015 Commerce Drive, Suite 450, Irving TX 75063 (214) 753-1127, (800) 367-4598	Locks and key control equipment
ADT Security Services, Inc., 1400 East Exposition Avenue, Aurora, CO 80012-2512, (303) 338-8200, (800) 662-5378	Electronic security products and services
AES Corporation, 285 Newbury Street, P.O. Box 2093, Peabody, MA 01960, (506) 535-7310, (800) 237-6387	Central alarm reporting systems
Allsafe Company, Inc., 1105 Broadway, Buffalo, NY 14212, (716) 896-4515, (800) 828-7162	Access control cards and systems
American Lock Co., 3400 W. Exchange Road, Crete, IL 60417, (708) 534-2000, (800) 323-4568	Padlocks, hasps, and cam locks
Apollo, 3610 Birch Street, Newport Beach, CA 92660, (714) 852-8178	Access control products, alarm panels, readers, software, and badging systems
Applied Real-time Systems, Inc., 1700 Highway 59, Mandeville, LA 70448, (504) 626-1111, (800) 256-2003	Hardware and software for access control
Arrow Lock, 103-00 Forster Avenue, Brooklyn, NY 11236, (718) 257-4700	Locks, key control software, interchangeable core products
ASSA High Security Locks, 10300 Foster Avenue, Brooklyn, NY 11236, (718) 927-2772, (800) 221-6529	Mechanical locks and key-making equipment
Best Access Systems, 6161 East 75th Street, P.O. Box 50444, Indianapolis, IN 46250 (317) 849-2250	Locks, access control equipment, key control and management software
Cardkey Systems, Inc., 1757 Tapo Canyon Road, Simi Valley, CA 93063, (805) 522-5555	Card-reader systems, computer-based access control systems
Casi-Rusco, 1155 Broken Sound Parkway NW, Boca Raton, FL 33487, (561) 998-6100	Integrated access control systems
Chubb Lock and Safe, 42 Shaft Road, Rexdale, ON M9W 4M2 Canada, (416) 249-7241	Locks, door hardware, access control systems, electric locks, vaults, and safes
Continental Instruments Corp., 70 Hopper Street, Westbury, NY 11590, (516) 334-0900	Card-reader systems, computer-based access control systems, electronic door locks
Control Systems International, Inc., 1625 West Crosby Road, Carrollton, TX 75007, (972) 323-1111, (800) 274-5551	Access control systems
Controlled Access, Inc., 1256 North Church Street, Suite D, Moorestown, NJ 08057, (609) 866-5525, (800) 377-5050	Computer-based access control systems
CorKey Control Systems, Inc., 3427 Enterprise, Hayward, CA 94545-3201, (510) 786-4241, (800) 622-2239	Magnetic locking hardware
Dayton Safe Company, 30 Kiser Street, Dayton, OH 45404, (937) 461-3900	Safes, lockers, and safety deposit boxes

MANUFACTURER/ADDRESS/PHONE	PRODUCTS
Del Norte Security Systems, 2922 South Roosevelt Street, Tempe, AZ 85282-2042, (602) 894-1731	Computerized card-reader systems
Elbex America, Inc., 10761 Noel Street, Los Alamitos, CA 90720, (714) 761-8000, (800) 367-2288	Audio and video equipment and door-entry control systems
Esmet, 1406 5th St. SW, Canton, OH 44712, (800) 321-0870	Mechanical locks and storage containers
Essex Electronics, Inc., 1130 Mark Avenue, Carpinteria, CA 93013, (805) 684-7601, (800) 628-9673	Keyless entry systems and touchpads
Folger Adam Security, Inc., 16300 West 103rd, Lemont, IL 60439, (630) 739-3900, (800) 966-6739	Door devices, locks, security hardware, and electric strikes
Galaxy Control Systems, P.O. Box 158, Walkersville, MD 21793-0158, (301) 845-6600, (800) 445-5560	Integrated access control and security management systems
Hamilton Products Group, Inc., P.O. Box 6248, Arlington, VA 22206-0248, (703) 527-8484, (800) 876-6066	GSA-approved containers and security filing cabinets
Hirsch Electronics Corporation, 2941 Alton Parkway, Irvine, CA 92606, (714) 250-8888	Access control systems, management software for access control, and scramble keypad systems
HPC, Inc., 3999 North 25th Avenue, Schiller Park, IL 60176, (708) 671-6280	Lock code, master keying, and key control software, and key control cabinets
Ilco Unican Corporation, 400 Jeffreys Road, P.O. Box 2627, Rocky Mount, NC 27802-2627, (919) 446-3321, (800) 334-1381	Access control systems (both electronic and mechanical) and locksmithing supplies
Intercon Security LTD., 40 Sheppard Avenue West, Toronto, ON M2N 6K9 Canada, (416) 229-6811	Access control systems
KABA High Security Locks, P.O. Box 490, Southington, CT 06489, (203) 621-3601	Patented high-security keying systems
Kastle Systems, Inc., 1501 Wilson Boulevard, Arlington, VA 22209, (703) 528-8800	Central station computer-controlled security for commercial office buildings
Key Systems, Inc., 948 Culver Road, Rochester, NY 14609, (716) 654-9388, (800) 888-3553	Key storage and control systems with access control
Keysure, P.O. Box 362, Hudson, New York, NY 12534, (518) 828-5337, (800) 803-7308	Key control containers and keyless lockboxes
KeyTrak, Inc., 1750 West Broadway, Suite 220, Orlando, FL 32765, (407) 366-5700, (800) 541-5033	Electronic key control with access control
Knox Company, 17672 Armstrong, Irvine, CA 92714, (714) 252-8181, (800) 552-5669	Rapid-entry systems, key control equipment, locks, and containers
LockSoft, Inc., P.O. Box 129, Hastings, NE 68901, (402) 461-4149	Key control and master-keying software
Master Lock Company, 2600 North 32nd Street, P.O. Box 10367, Milwaukee, WI 53210, (414) 444-2800	Mechanical locks

MANUFACTURER/ADDRESS/PHONE	PRODUCTS
Mastiff Electronic Systems, 1698 Sands Place, Suite D, Marietta, GA 30067, (770) 984-0202	Coded, hands-off, access control
Matrix Systems, Inc., 7550 Paragon Road, Dayton, OH 45459, (513) 438-9033, (800) 562-8749	Card-reader systems and systems integration
Maxton Security Systems, 5658-1 Etiwanda Avenue, Tarzana, CA 91356, (818) 776-8557	Office protection devices, file cabinets, and lock boxes
Medeco Security Locks, Inc., P.O. Box 3075, Salem, VA 24153, (530) 380-5000 West Salem, VA 24153, (703) 380-5000	High-security locks, filing cabinets, and key cabinets
MMF - Major Metalfab Co., 370 Alice Street, Wheeling, IL 60090, (847) 537-7890, (800) 323-8181	Containers, key control equipment, and seals
Morse Watchman, Inc., 2 Morse Road, Oxford, CT 06478, (203) 264-4949, (800) 423-8256	Key control systems and equipment
Mosler, Inc., 8509 Berk Boulevard, Hamilton, OH 45015-2213, (800) 667-5371	Access control systems, GSA-approved security filing cabinets, containers (including key control), and vaults
MRL Security, 7644 Fullerton Road, Springfield, VA 22153, (703) 569-0195, (800) 989-9891	Access control systems
Northern Computers, Inc., 5007 South Howell Avenue, Milwaukee, WI 53207, (414) 769-5980, (800) 323-4576	Access control systems, identification equipment, and video badging systems
Receptors, Inc., 455 Maple Avenue, Torrance, CA 90503, (310) 781-7878	Computer-based access control systems
RJR Software, 7 Kaffir Lily Place, Palm Coast, FL 32164, (904) 437-1162	Security control software
Safemasters Company, Inc., 2700 Garfield Avenue, Silver Springs, MD 20910, (301) 608-9000, (800) 480-1845	Security services, electronic and mechanical security equipment, access control and computerized master-keying systems
Sargent and Greenleaf, Inc., 1 Security Drive, Nicholasville, KY 40356, (606) 887-9411	Access control systems, banking security equipment, and locks
Schlage Lock Company, 2401 Bayshore Boulevard, P.O. Box 193324, San Francisco, CA 94134, (415) 330-5530	Access control equipment and locks
Securitech Group, Inc., 54-45 44th Street, Maspeth, NY 11378-1031, (718) 392-9000, (800) 622-5625	Access control equipment, security doors, and locks
Securitron Magnalock Corporation, 550 Vista Boulevard, Sparks, NV 89434-6632, (702) 355-5625, (800) 624-5625	Electromagnetic locking devices and access control systems
Sensormatic Electronics Corporation, 951 Yamato Road, Boca Raton, FL 33431, (561) 989-7000, (800) 368-7262	Integrated access control and identification systems
Simplex, 1 Simplex Plaza, Gardner, MA 01441, (508) 632-2500	Mechanical pushbutton combination locks

MANUFACTURER/ADDRESS/PHONE	PRODUCTS
Synergistics, Inc., 9 Tech Circle, Natick, MA 01760, (508) 655-1340	Card-reader systems, computer-based access control systems
Supra Products, Inc., 2611 Pringle Road SE, P.O. Box 3167, Salem, OR 97302-0167, (503) 581-9101, (800) 905-3226	Electronic access control (combined with mechanical key control) and access activity tracking
Telkee, 60 Starlifter Avenue, Kent County Aeropark, Dover, DE 19901, (302) 678-7800	Indexed key control containers and systems
Treskat USA, 725 Adriane Park Circle, Kissimmee, FL 34744, (407) 870-9696, (800) 645-5657	Key control and key management software for locksmiths
Trigon Electronics, 1220 North Batavia Street, Orange, CA 92667, (714) 633-7442	Telephone control systems and card-reader systems
Vikonics, Inc., P.O. Box 2168, South Hackensack, NJ 07606-2168, (201) 641-8077, (800) 626-5416	Computer-based access control systems
Yale Security, Inc., P.O. Box 25288, Charlotte, NC 28229-8010, (704) 283-2101, Ext. 140, (800) 438-1951	Mechanical and electronic operating locks

APPENDIX G

CHECKLISTS FOR LOCK AND KEY CONTROL

CHECKLIST FOR LOCK AND KEY CONTROL*

1. Are the number of individuals with the entry code to the facility or who possess keys kept to a minimum?
2. Are locks re-keyed or codes changed for the facility when an individual leaves or a key is lost or a code compromised?
3. Is the code on keypads or mechanical access control systems (key locks, pushbutton locks, etc.) changed on a regular basis?
4. Is there a procedure in place for controlling badges, keys, combinations, and/or cards used for entry to the facility?
5. Is a policy in place on the dissemination of access control devices listed in question 4 and a policy for replacing them when they are lost?
6. When an individual's facility entry authority is revoked is there policy in place to:
    A. Revise authorization lists?
    B. Change locks/combinations?
    C. Surrender badges, keys and/or cards?
7. Is access to facility resources denied quickly enough to prevent damage to resources by a person whose facility entry authorization has been revoked?
8. Have procedures been developed for lock and key control?
9. Has someone been assigned responsibility for lock and key control oversight?
10. Is the total number of keys issued known and documented?
11. Is the total number of master keys issued known and documented?
12. Has criteria been developed for issuing keys and/or access cards?
13. Are key inventories conducted on a regular basis?
14. Are key holders specifically instructed not to duplicate keys?
15. Is there a central location for duplicating keys?
16. Are all keys marked "Do not duplicate"?
17. Are key blanks and keys not in use stored in a lockable, key security control box?
18. Are all keys to the key security control box accounted for?
19. Are individuals assigned specific responsibility for the keys to the key security control box?
20. Is there a facility key access/issuance log?
21. Is the key access/issuance log located in a secured area?
22. Are the key access/issuance logs reviewed on a regular basis?
23. Are keys attended at all times?
24. Is there an established key return system for terminated, suspended, or resigning employees?
25. Has someone been assigned responsibility for locksmith duties?
26. Does the facility have a locksmith on duty? On the facility payroll?
27. If not, does the facility have an agreement with a locksmith service to provide services on a contingency basis?
28. Are facility locks inspected for functionality?
29. Has an inspection been done within the last year?
30. Were all locks found to be operating correctly at the time of the inspection?
31. Are keys accessible only to those individuals whose duties require access to them?
32. Is there a policy in place for determining if an individual currently requires access to keys?

33. Are keypad-viewing shields used to deny unauthorized observation of entry codes?
34. Are doors locked when not in use?
35. Are employees discouraged from holding secured doors open for others or allowing follow-ins?
36. Are procedures in place to prevent tailgating?
37. Are padlocks locked to hasp when not in use?
38. Are locks and frames designed to prohibit the forced spreading of doorframes (e.g., metal jimmy guards)?

*If the answer to any of these questions is "no," action should be taken to correct the problem immediately. See Chapter 3 for further guidance.

CHECKLIST FOR ARMS AMMUNITION AND EXPLOSIVES (AA&E) LOCK AND KEY CONTROL*

1. Are keys to areas protecting AA&E maintained separately from all other keys?
2. Are keys issued to personnel only from authorized access lists?
3. Are authorized access lists not available to unauthorized individuals?
4. Is the number of keys issued for any single lock held to a minimum?
5. Are keys that haven't been issued always attended?
6. Are keys that haven't been issued always secured?
7. For Category III and IV AA&E, are designated key storage containers at least 20-gauge steel construction, have a UL 768 listed built-in, Group 1 changeable combination lock or a GSA-approved combination padlock (S&G Model 8077)?
8. Are keys to Category I and II AA&E stored in a Class 5 GSA-approved security container?
9. Do keys always remain at the facility?
10. Are keys restricted from remaining with any one individual during operations or overnight?
11. Are keys returned immediately after the storage facility is secured?
12. Are high-security locks rotated or re-keyed at least annually?
13. Are high-security locks replaced immediately when keys are lost, misplaced, or stolen?
14. Are replacement or reserve locks, cores, cylinders, and keys secured in designated key storage containers or a Class 5 GSA-approved container to prevent access by unauthorized individuals?
15. Does each lock on a storage facility operate only with its own change key (no master keying or keying alike is allowed)?
16. Is a lock and key custodian appointed and designated in writing?
17. Is a key control log maintained to ensure key accountability (Table E-3 in Appendix E)?
18. Are accountability records retained for 90 days?
19. Are padlocks always locked to the staple or hasp when the door or container is open?
20. Are inventories of keys and locks conducted semiannually?
21. Is positive, two-person control required for entry into Category I through IV magazine and storage facilities?

*If the answer to any of these questions is "no," action should be taken to correct the problem immediately. See Chapter 5 for further guidance.

CHECKLIST FOR CHEMICAL AND SPECIAL WEAPONS (C&SW) LOCK AND KEY CONTROL*

In addition to the checklist for AA&E, the following apply specifically to the protection of C&SW:

1. Are keys to chemical or special storage facilities controlled as classified material and stored in a Class 5 security container?
2. Are keys stored separately from all other keys?
3. Are keys and locks audited monthly?
4. Are keys inventoried with each change of custody?
5. Is positive two-person control used for access to all C&SW storage facilities?
6. Is a two-key entry system (two separate locking systems or one locking system with two keys) used to ensure compliance with the two-person requirement?

*If the answer to any of these questions is "no," action should be taken to correct the problem immediately. See Chapter 5 for further guidance.